日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ２月２３日

出願番号
Application Number: 特願２００１－０４８９１６

出願人
Applicant(s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ５月３０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特２００１－３０４７３４７

【書類名】　特許願
【整理番号】　0100042207
【提出日】　平成13年 2月23日
【あて先】　特許庁長官　及川　耕造　殿
【国際特許分類】　H04K　1/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　大嶋　拓哉
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　大塚　武
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　本城　哲
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　荒川　真志
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100095957
　【弁理士】
　【氏名又は名称】　亀谷　美明

【電話番号】　03-3226-6631

【先の出願に基づく優先権主張】

【出願番号】　特願2000-142307

【出願日】　平成12年 5月10日

【手数料の表示】

【予納台帳番号】　040224

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0012374

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子決済システム，決済管理装置，店舗装置，クライアント装置，ＩＣカード，コンピュータプログラムおよび記憶媒体

【特許請求の範囲】

【請求項１】　価値情報が記憶されたＩＣカードと，前記ＩＣカードに対する情報入出力機能を備えたクライアント装置と，商品またはサービスを提供する店舗装置と，前記ＩＣカードと前記店舗装置間の決済を管理する決済管理装置と，前記クライアント装置と前記店舗装置と前記決済管理装置とを双方向通信可能に接続する通信系とから成る電子決済システムであって，

前記決済管理装置は，前記ＩＣカードで決済を行うための決済情報を，前記店舗装置からの決済要求情報に基づいて生成し，前記決済情報を前記決済管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された決済情報を前記クライアント装置に送信し，

前記クライアント装置は，前記決済管理装置から受信した前記決済情報を前記ＩＣカードに出力することを特徴とする，電子決済システム。

【請求項２】　前記店舗装置は，前記決済要求情報の正当性を示す第１署名を前記店舗装置の秘密鍵を用いて作成し，前記第１署名が付された前記決済要求情報を前記決済管理装置に送信し，

前記決済管理装置は，前記店舗装置から受信した前記第１署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項１記載の電子決済システム。

【請求項３】　前記第１署名が付された前記決済要求情報は，前記クライアント装置を介して前記決済管理装置に送信されることを特徴とする，請求項２記載の電子決済システム。

【請求項４】　前記決済管理装置は，前記第１署名付き決済情報の正当性を示す第２署名を前記決済管理装置の秘密鍵を用いて作成し，この第２署名が付され暗号化された前記決済情報を前記クライアント装置に送信し，

前記クライアント装置は，前記決済管理装置から受信した前記第２署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に，前記決

済情報を前記ＩＣカードに出力することを特徴とする，請求項２記載の電子決済システム。

【請求項５】　前記決済管理装置は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を前記決済管理装置の秘密鍵を用いて生成し，前記決済情報を含むとともにこの第３署名が付された前記決済完了情報を前記店舗装置に送信し，

前記店舗装置は，前記決済管理装置から受信した前記第３署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項１記載の電子決済システム。

【請求項６】　前記店舗装置は，前記第３署名が付された決済完了情報を受信し，前記店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報を前記決済管理装置および前記クライアント装置に送信し，

前記決済管理装置および前記クライアント装置は，前記店舗装置から受信した前記第４署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項第５記載の電子決済システム。

【請求項７】　前記店舗装置は，複数の下層店舗装置を含むモールとして構成されていることを特徴とする，請求項１記載の電子決済システム。

【請求項８】　ＩＣカードに記憶されている価値情報をクライアント装置を介して更新することが可能な決済管理装置において，

前記決済管理装置は，前記ＩＣカードの価値更新情報を前記決済管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された価値更新情報を前記クライアント装置に送信し，

前記クライアント装置は，受信した前記価値更新情報を前記ＩＣカードに入力することを特徴とする，決済管理装置。

【請求項９】　前記決済管理装置は，前記価値更新情報の正当性を示す第５署名を前記決済管理装置の秘密鍵を用いて生成し，前記第５署名が付された前記価値更新情報を前記クライアント装置に送信し，

前記クライアント装置は，前記決済管理装置から受信した前記第５署名の正当

性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に，前記価値更新情報を前記ＩＣカードに入力することを特徴とする，請求項８記載の決済管理装置。

【請求項１０】　価値情報が記憶されたＩＣカードと商品またはサービスを提供する店舗装置との間の決済を管理する決済管理装置において，

前記ＩＣカードで決済を行うための決済情報を，前記店舗装置からの決済要求情報に基づいて生成する決済情報生成部と，

前記決済情報を前記決済管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化する決済情報暗号化部と，

この暗号化された決済情報を前記ＩＣカードに対する情報入出力機能を備えたクライアント装置を介して前記ＩＣカードに出力する決済情報出力部とを備えたことを特徴とする，決済管理装置。

【請求項１１】　前記店舗装置は，前記決済要求情報の正当性を示す第１署名を前記店舗装置の秘密鍵を用いて作成し，前記第１署名が付された前記決済要求情報を前記決済管理装置に送信し，

前記決済管理装置は，前記店舗装置から受信した前記第１署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項１０記載の決済管理装置。

【請求項１２】　前記決済管理装置は，前記第１署名付き決済情報の正当性を示す第２署名を前記決済管理装置の秘密鍵を用いて作成し，この第２署名が付され暗号化された前記決済情報を，前記第２署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証可能な前記クライアント装置に送信して前記ＩＣカードに出力することを特徴とする，請求項１１記載の決済管理装置。

【請求項１３】　前記決済管理装置は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を前記決済管理装置の秘密鍵を用いて生成し，前記決済情報を含むとともにこの第３署名が付された前記決済完了情報を，前記第３署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証可能な前記店舗装置に送信することを特徴とする，請求項１０記載の決済管理装置。

【請求項１４】　前記店舗装置は，前記第３署名が付された決済完了情報を

受信し，前記店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報を前記決済管理装置に送信し，

前記決済管理装置は，前記店舗装置から受信した前記第４署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項第１３記載の決済管理装置。

【請求項１５】　コンピュータをして請求項８記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項１６】　コンピュータをして請求項９記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項１７】　コンピュータをして請求項１０記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項１８】　コンピュータをして請求項１１記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項１９】　コンピュータをして請求項１２記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項２０】　コンピュータをして請求項１３記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項２１】　コンピュータをして請求項１４記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項２２】　請求項１５記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項２３】　請求項１６記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項２４】　請求項１７記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項２５】　請求項１８記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項２６】　請求項１９記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項２７】　請求項２０記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項２８】　請求項２１記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項２９】　決済管理装置を介して価値情報が記憶されたＩＣカードとの間で行われる決済に基づいて，商品またはサービスを提供する店舗装置であって，

決済要求情報を生成する決済要求情報生成部と，

前記決済要求情報の正当性を示す第１署名を前記店舗装置の秘密鍵を用いて作成する第１署名生成部と，

前記第１署名が付された前記決済要求情報を，前記第１署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証可能な前記決済管理装置に送信する決済要求情報送信部とを備えたことを特徴とする，店舗装置。

【請求項３０】　前記決済管理装置は，前記ＩＣカードで決済を行うための決済情報を，前記店舗装置からの決済要求情報に基づいて生成し，前記決済情報を前記決済管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された決済情報を前記クライアント装置に送信し，

前記クライアント装置は，前記決済管理装置から受信した前記決済情報を前記ＩＣカードに出力することを特徴とする，請求項２９記載の店舗装置。

【請求項３１】　前記第１署名が付された前記決済要求情報は，前記店舗装置から前記クライアント装置を介して前記決済管理装置に送信されることを特徴とする，請求項２９記載の店舗装置。

【請求項３２】　前記決済管理装置は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を前記決済管理装置の秘密鍵を用いて生成し，前記決済情報を含むとともにこの第３署名が付された前記決済完了情報を前記店舗装置に送信し，

前記店舗装置は，前記決済管理装置から受信した前記第３署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項２９記載の店舗装置。

【請求項３３】　前記店舗装置は，前記第３署名が付された決済完了情報を受信し，前記店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報を前記決済管理装置および前記クライアント装置に送信し，

前記決済管理装置および前記クライアントは，前記店舗装置から受信した前記第４署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項第３２記載の店舗装置。

【請求項３４】　前記店舗装置は，複数の下層店舗装置を含むモールとして構成されていることを特徴とする，請求項２９記載の店舗装置。

【請求項３５】　コンピュータをして請求項２９記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項３６】　コンピュータをして請求項３０記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項３７】　コンピュータをして請求項３１記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項３８】　コンピュータをして請求項３２記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項３９】　コンピュータをして請求項３３記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項４０】　コンピュータをして請求項３４記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項４１】　請求項３５記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項４２】　請求項３６記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項４３】　請求項３７記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項４４】　請求項３８記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項４５】　請求項３９記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項４６】　請求項４０記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項４７】　商品またはサービスを提供する店舗装置と価値情報が記憶されたＩＣカードとの間の決済を決済管理装置を介して行うに際して使用される前記ＩＣカードに対する情報入出力機能を備えたクライアント装置において，

前記決済管理装置が，前記店舗装置からの決済要求情報に基づいて生成し，前記決済管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化した決済情報を受信する決済情報受信部と，

前記決済管理装置から受信した前記決済情報を前記ＩＣカードに出力する決済情報出力部とを備えていることを特徴とする，クライアント装置。

【請求項４８】　前記店舗装置は，前記決済要求情報の正当性を示す第１署名を前記店舗装置の秘密鍵を用いて作成し，前記第１署名が付された前記決済要求情報を前記クライアント装置を介して前記決済管理装置に送信し，

前記決済管理装置は，前記店舗装置から受信した前記第１署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項４７記載のクライアント装置。

【請求項４９】　前記決済管理装置は，前記第１署名付き決済情報の正当性を示す第２署名を前記決済管理装置の秘密鍵を用いて作成し，この第２署名が付され暗号化された前記決済情報を前記クライアント装置に送信し，

前記クライアント装置は，前記決済管理装置から受信した前記第２署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に，前記決済情報を前記ＩＣカードに出力することを特徴とする，請求項４８記載のクライアント装置。

【請求項５０】　前記決済管理装置は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を前記決済管理装置の秘密鍵を用いて生成し，前記決済情報を含むとともにこの第３署名が付された前記決済完了情報を前記店舗装置に送信し，

前記店舗装置は，前記決済管理装置から受信した前記第３署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証し，さらに前記店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報を前記クライアント装置に送信し，

前記クライアントは，前記店舗装置から受信した前記第４署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項第４７記載のクライアント装置。

【請求項５１】　コンピュータをして請求項４７記載のクライアント装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項５２】　コンピュータをして請求項４８記載のクライアント装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項５３】　コンピュータをして請求項４９記載のクライアント装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項５４】　コンピュータをして請求項５０記載のクライアン装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項５５】　請求項５１記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項５６】　請求項５２記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項５７】　請求項５３記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項５８】　請求項５４記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項５９】　商品またはサービスを提供する店舗装置との間の決済を決済管理装置を介して行うに際して使用される価値情報が記憶されたＩＣカードにおいて

前記決済管理装置が，前記店舗装置からの決済要求情報に基づいて生成し，前記決済管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化した決済情報を，前記ＩＣカードに対する情報入出力機能を備えた前記クライアント

装置を介して入力可能であることを特徴とする，ＩＣカード。

【請求項６０】　前記店舗装置は，前記決済要求情報の正当性を示す第１署名を前記店舗装置の秘密鍵を用いて作成し，前記第１署名が付された前記決済要求情報を前記決済管理装置に送信し，

前記決済管理装置は，前記店舗装置から受信した前記第１署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証するとともに，前記第１署名付き決済情報の正当性を示す第２署名を前記決済管理装置の秘密鍵を用いて作成し，この第２署名が付され暗号化された前記決済情報を前記クライアント装置に送信し，

前記クライアント装置は，前記決済管理装置から受信した前記第２署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に，前記決済情報を前記ＩＣカードに出力することを特徴とする，請求項５９記載のＩＣカード。

【請求項６１】　価値情報が記憶されたＩＣカード手段と，

前記ＩＣカードに対する情報入出力機能を備えたクライアント手段と，

商品またはサービスを提供する店舗手段であって，クライアント手段からの購入要求に応じて前記ＩＣカードによる決済情報を生成する店舗手段と，

前記ＩＣカードと前記店舗手段間の決済を管理する決済管理手段であって，前記ＩＣカードで決済を行うための決済情報を，前記店舗手段からの決済要求情報に基づいて生成し，前記決済情報を前記決済管理手段と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された決済情報を前記クライアント手段に送信する決済管理手段と，

前記クライアント手段と前記店舗手段と前記決済管理手段とを双方向通信可能に接続する通信系とから成ることを特徴とする，電子決済システム。

【請求項６２】　前記店舗手段は，前記決済要求情報の正当性を示す第１署名を前記店舗手段の秘密鍵を用いて作成し，前記第１署名が付された前記決済要求情報を前記決済管理手段に送信し，

前記決済管理手段は，前記店舗手段から受信した前記第１署名の正当性を前記店舗手段の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項

６１記載の電子決済システム。

【請求項６３】　前記第１署名が付された前記決済要求情報は，前記クライアント手段を介して前記決済管理手段に送信されることを特徴とする，請求項６２記載の電子決済システム。

【請求項６４】　前記決済管理手段は，前記第１署名付き決済情報の正当性を示す第２署名を前記決済管理手段の秘密鍵を用いて作成し，この第２署名が付され暗号化された前記決済情報を前記クライアント手段に送信し，

前記クライアント手段は，前記決済管理手段から受信した前記第２署名の正当性を前記決済管理手段の秘密鍵に対応する公開鍵を用いて検証した後に，前記決済情報を前記ＩＣカードに出力することを特徴とする，請求項６２記載の電子決済システム。

【請求項６５】　前記決済管理手段は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を前記決済管理手段の秘密鍵を用いて生成し，前記決済情報を含むとともにこの第３署名が付された前記決済完了情報を前記店舗手段に送信し，

前記店舗手段は，前記決済管理手段から受信した前記第３署名の正当性を前記決済管理手段の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項６１記載の電子決済システム。

【請求項６６】　前記店舗手段は，前記第３署名が付された決済完了情報を受信し，前記店舗手段の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報を前記決済管理手段および前記クライアント手段に送信し，

前記決済管理手段および前記クライアントは，前記店舗手段から受信した前記第４署名の正当性を前記店舗手段の秘密鍵に対応する公開鍵を用いて検証することを特徴とする，請求項第６１記載の電子決済システム。

【請求項６７】　前記店舗手段は，複数の下層店舗手段を含むモールとして構成されていることを特徴とする，請求項６１記載の電子決済システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】　本発明は，共通鍵を保持したＩＣカードを用いて，ネットワークなどを用いた決済処理を安全に行うことができる電子決済システム，決済管理装置，店舗装置，クライアント装置，ＩＣカード，コンピュータプログラムおよび記憶媒体に関する。

【０００２】

【従来の技術】　インターネットなどのオープンネットワークを介した電子商取引を安全に行うために，従来，ＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ：公開鍵インフラ）プロトコルが採用されている。

【０００３】

ＰＫＩプロトコルでは，送信元で秘密鍵を用いて署名情報を作成し，送信元から送信先に，当該署名情報を伝送情報と共に送信する。そして，送信先において，当該秘密鍵に対応する公開鍵を用いて当該署名情報の検証を行うことで，受信した伝送情報が正当な送信元で作成されたものであるか否かを判断する。

【０００４】

ところで，近年，ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）カードを用いて，ネットワークを介した電子商取引を行う試みがある。ここで，通常，ＩＣカードは，共通鍵を保持しており，共通鍵暗号方式を用いて秘匿性のある情報の入出力を行う。このようなＩＣカードは，共通鍵が署名情報を作成するための鍵とはなり得ないため，ＩＣカードを紛失した場合でも，被害を小さくできるという利点がある。

【０００５】

【発明の解決しようとする課題】　しかしながら，ネットワークを介した電子商取引を安全に行うためには，秘密鍵を用いて署名情報を作成する必要があるが，従来の手法では，ＩＣカードが秘密鍵を保持（記憶）していないため，署名情報の作成ができないという問題がある。この場合に，ＩＣカードに秘密鍵を保持する方法も考えられるが，前述したように，秘密鍵は署名情報を作成できるため印鑑照明と同様の効力があり，ＩＣカードを紛失して悪用されたときの被害が大きすぎるという問題がある。

【０００６】

また，上述したようなＩＣカードが採用する共通鍵暗号方式のみを用いて，ネットワークを介した電子商取引を行うと，取り引きを行う多数の相手先のサーバ装置などが共通鍵を持つことになり，共通鍵が盗まれたり，悪用される可能性が高くなるという問題もある。

【０００７】

従来の電子決済においては，ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）やＳＥＴ（Ｓｅｃｕｒｅ　Ｅｌｅｃｔｒｏｎｉｃ　Ｔｒａｎｓａｃｔｉｏｎ）が多く採用されている。しかし，ＳＳＬでは，クライアント装置と店舗装置間の通信路に対する安全性は保証されるが，店舗側の不正を検出できないという問題がある。

【０００８】

また，ＳＥＴでは，ＳＳＬの利点とクライアント装置，店舗装置，決済管理装置で改ざんができないという利点とを併せ持つが，各装置がＰＫＩの証明書を持たなければならないため，煩雑であり費用がかかり，さらに署名および署名検証を何度も行わなければならず冗長であるという問題がある。

【０００９】

さらに，従来の電子商取引システムにおいては，ユーザがクライアント装置上で確認した価値情報が，実際にＩＣカードに書き込まれる価値情報と同じであるかどうかを確認する手段を持っていなかった。

【００１０】

本発明は上述した従来技術の問題点に鑑みてなされ，共通鍵を保持したＩＣカードを用いて，ネットワークを介した電子商取引を安全に行うことができる電子決済システム，決済管理装置，店舗装置，クライアント装置，ＩＣカード，コンピュータプログラムおよび記憶媒体を提供することを目的とする。

【００１１】

【課題を解決するための手段】

上記課題を解決するために，本発明によれば，新規かつ改良された電子決済システム，決済管理装置，店舗装置，クライアント装置，ＩＣカード，コンピュータプログラムおよび記憶媒体が提供される。

【００１２】

本発明の第１の観点によれば，価値情報が記憶されたＩＣカードと，ＩＣカードに対する情報入出力機能を備えたクライアント装置と，商品またはサービスを提供する店舗装置と，ＩＣカードと店舗装置間の決済を管理する決済管理装置と，クライアント装置と店舗装置と決済管理装置とを双方向通信可能に接続する通信系とから成る電子決済システムであって，決済管理装置は，ＩＣカードで決済を行うための決済情報を，店舗装置からの決済要求情報に基づいて生成し，決済情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された決済情報をクライアント装置に送信し，クライアント装置は，決済管理装置から受信した決済情報をＩＣカードに出力することを特徴とする，電子決済システムが提供される。

【００１３】

上記電子決済システムにおいて，店舗装置は，決済要求情報の正当性を示す第１署名を店舗装置の秘密鍵を用いて作成し，第１署名が付された決済要求情報を決済管理装置に送信し，決済管理装置は，店舗装置から受信した第１署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００１４】

第１署名が付された決済要求情報は，クライアント装置を介して決済管理装置に送信されることが好ましい。

【００１５】

決済管理装置は，第１署名付き決済情報の正当性を示す第２署名を決済管理装置の秘密鍵を用いて作成し，この第２署名が付され暗号化された決済情報をクライアント装置に送信し，クライアント装置は，決済管理装置から受信した第２署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に，決済情報をＩＣカードに出力することが好ましい。

【００１６】

決済管理装置は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を決済管理装置の秘密鍵を用いて生成し，決済情報を含むとともにこの第３署名が付された決済完了情報を店舗装置に送信し，

【００１７】

店舗装置は，決済管理装置から受信した第３署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００１８】

店舗装置は，第３署名が付された決済完了情報を受信し，店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報を決済管理装置およびクライアント装置に送信し，決済管理装置およびクライアント装置は，店舗装置から受信した第４署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００１９】

店舗装置は，単一の店舗装置として構成しても良いし，複数の下層店舗装置を含むモールとして構成しても良い。

【００２０】

さらに本発明の別の観点によれば，ＩＣカードに記憶されている価値情報をクライアント装置を介して更新することが可能な決済管理装置において，決済管理装置は，ＩＣカードの価値更新情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された価値更新情報をクライアント装置に送信し，クライアント装置は，受信した価値更新情報をＩＣカードに入力することを特徴とする，決済管理装置が提供される。

【００２１】

決済管理装置は，価値更新情報の正当性を示す第５署名を決済管理装置の秘密鍵を用いて生成し，第５署名が付された価値更新情報をクライアント装置に送信し，クライアント装置は，決済管理装置から受信した第５署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に，価値更新情報をＩＣカードに入力することが好ましい。

【００２２】

価値情報が記憶されたＩＣカードと商品またはサービスを提供する店舗装置との間の決済を管理する決済管理装置において，ＩＣカードで決済を行うための決済情報を，店舗装置からの決済要求情報に基づいて生成する決済情報生成部と，

決済情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化する決済情報暗号化部と，この暗号化された決済情報をＩＣカードに対する情報入出力機能を備えたクライアント装置を介してＩＣカードに出力する決済情報出力部とを備えたことが好ましい。

【００２３】

店舗装置は，決済要求情報の正当性を示す第１署名を店舗装置の秘密鍵を用いて作成し，第１署名が付された決済要求情報を決済管理装置に送信し，決済管理装置は，店舗装置から受信した第１署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００２４】

決済管理装置は，第１署名付き決済情報の正当性を示す第２署名を決済管理装置の秘密鍵を用いて作成し，この第２署名が付され暗号化された決済情報を，第２署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証可能なクライアント装置に送信してＩＣカードに出力することが好ましい。

【００２５】

決済管理装置は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を決済管理装置の秘密鍵を用いて生成し，決済情報を含むとともにこの第３署名が付された決済完了情報を，第３署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証可能な店舗装置に送信することが好ましい。

【００２６】

店舗装置は，第３署名が付された決済完了情報を受信し，店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報を決済管理装置に送信し，決済管理装置は，店舗装置から受信した第４署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００２７】

さらに，本発明の別の観点によれば，コンピュータをして上記決済管理装置として機能せしめることを特徴とするコンピュータプログラムが提供される。

【００２８】

また，本発明の別の観点によれば，コンピュータをして上記決済管理装置として機能せしめることを特徴とする上記コンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体が提供される。

【００２９】

さらにまた，本発明の別の観点によれば，決済管理装置を介して価値情報が記憶されたＩＣカードとの間で行われる決済に基づいて，商品またはサービスを提供する店舗装置であって，決済要求情報を生成する決済要求情報生成部と，決済要求情報の正当性を示す第１署名を店舗装置の秘密鍵を用いて作成する第１署名生成部と，第１署名が付された決済要求情報を，第１署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証可能な決済管理装置に送信する決済要求情報送信部とを備えたことを特徴とする，店舗装置が提供される。

【００３０】

決済管理装置は，ＩＣカードで決済を行うための決済情報を，店舗装置からの決済要求情報に基づいて生成し，決済情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された決済情報をクライアント装置に送信し，クライアント装置は，決済管理装置から受信した決済情報をＩＣカードに出力することが好ましい。

【００３１】

第１署名が付された決済要求情報は，店舗装置からクライアント装置を介して決済管理装置に送信されることが好ましい。

【００３２】

決済管理装置は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を決済管理装置の秘密鍵を用いて生成し，決済情報を含むとともにこの第３署名が付された決済完了情報を店舗装置に送信し，店舗装置は，決済管理装置から受信した第３署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００３３】

店舗装置は，第３署名が付された決済完了情報を受信し，店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領

情報を決済管理装置およびクライアント装置に送信し，決済管理装置およびクライアントは，店舗装置から受信した第４署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００３４】

店舗装置は，単一の店舗装置として構成しても良いし，複数の下層店舗装置を含むモールとして構成しても良い。

【００３５】

さらに，本発明の別の観点によれば，コンピュータをして上記店舗装置として機能せしめることを特徴とするコンピュータプログラムが提供される。

【００３６】

また，本発明の別の観点によれば，コンピュータをして上記店舗装置として機能せしめることを特徴とする上記コンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体が提供される。

【００３７】

さらにまた，本発明の別の観点によれば，商品またはサービスを提供する店舗装置と価値情報が記憶されたＩＣカードとの間の決済を決済管理装置を介して行うに際して使用されるＩＣカードに対する情報入出力機能を備えたクライアント装置において，決済管理装置が，店舗装置からの決済要求情報に基づいて生成し，決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化した決済情報を受信する決済情報受信部と，決済管理装置から受信した決済情報をＩＣカードに出力する決済情報出力部とを備えていることを特徴とする，クライアント装置が提供される。

【００３８】

店舗装置は，決済要求情報の正当性を示す第１署名を店舗装置の秘密鍵を用いて作成し，第１署名が付された決済要求情報をクライアント装置を介して決済管理装置に送信し，決済管理装置は，店舗装置から受信した第１署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００３９】

決済管理装置は，第１署名付き決済情報の正当性を示す第２署名を決済管理装

置の秘密鍵を用いて作成し，この第２署名が付され暗号化された決済情報をクライアント装置に送信し，クライアント装置は，決済管理装置から受信した第２署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に，決済情報をＩＣカードに出力することが好ましい。

【００４０】

決済管理装置は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を決済管理装置の秘密鍵を用いて生成し，決済情報を含むとともにこの第３署名が付された決済完了情報を店舗装置に送信し，店舗装置は，決済管理装置から受信した第３署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証し，さらに店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報をクライアント装置に送信し，クライアントは，店舗装置から受信した第４署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００４１】

さらに，本発明の別の観点によれば，コンピュータをして上記クライアント装置として機能せしめることを特徴とするコンピュータプログラムが提供される。

【００４２】

また，本発明の別の観点によれば，コンピュータをして上記クライアント装置として機能せしめることを特徴とする上記コンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体が提供される。

【００４３】

さらに本発明の別の観点によれば，商品またはサービスを提供する店舗装置との間の決済を決済管理装置を介して行うに際して使用される価値情報が記憶されたＩＣカードにおいて，決済管理装置が，店舗装置からの決済要求情報に基づいて生成し，決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化した決済情報を，ＩＣカードに対する情報入出力機能を備えたクライアント装置を介して入力可能であることを特徴とする，ＩＣカードが提供される。

【００４４】

店舗装置は，決済要求情報の正当性を示す第１署名を店舗装置の秘密鍵を用い

て作成し，第１署名が付された決済要求情報を決済管理装置に送信し，決済管理装置は，店舗装置から受信した第１署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証するとともに，第１署名付き決済情報の正当性を示す第２署名を決済管理装置の秘密鍵を用いて作成し，この第２署名が付され暗号化された決済情報をクライアント装置に送信し，クライアント装置は，決済管理装置から受信した第２署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に，決済情報をＩＣカードに出力することが好ましい。

【００４５】

さらに，本発明の別の観点によれば，価値情報が記憶されたＩＣカード手段と，ＩＣカードに対する情報入出力機能を備えたクライアント手段と，商品またはサービスを提供する店舗手段であって，クライアント手段からの購入要求に応じてＩＣカードによる決済情報を生成する店舗手段と，ＩＣカードと店舗手段間の決済を管理する決済管理手段であって，ＩＣカードで決済を行うための決済情報を，店舗手段からの決済要求情報に基づいて生成し，決済情報を決済管理手段とＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された決済情報をクライアント手段に送信する決済管理手段と，クライアント手段と店舗手段と決済管理手段とを双方向通信可能に接続する通信系とから成ることを特徴とする，電子決済システムが提供される。

【００４６】

店舗手段は，決済要求情報の正当性を示す第１署名を店舗手段の秘密鍵を用いて作成し，第１署名が付された決済要求情報を決済管理手段に送信し，決済管理手段は，店舗手段から受信した第１署名の正当性を店舗手段の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００４７】

第１署名が付された決済要求情報は，クライアント手段を介して決済管理手段に送信されることが好ましい。

【００４８】

決済管理手段は，第１署名付き決済情報の正当性を示す第２署名を決済管理手段の秘密鍵を用いて作成し，この第２署名が付され暗号化された決済情報をクラ

イアント手段に送信し，クライアント手段は，決済管理手段から受信した第２署名の正当性を決済管理手段の秘密鍵に対応する公開鍵を用いて検証した後に，決済情報をＩＣカードに出力することが好ましい。

【００４９】

決済管理手段は，決済完了情報を生成し，この決済完了情報の正当性を示す第３署名を決済管理手段の秘密鍵を用いて生成し，決済情報を含むとともにこの第３署名が付された決済完了情報を店舗手段に送信し，

【００５０】

店舗手段は，決済管理手段から受信した第３署名の正当性を決済管理手段の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００５１】

店舗手段は，第３署名が付された決済完了情報を受信し，店舗手段の秘密鍵を用いて第４署名付き決済完了受領情報を生成し，この第４署名付き決済完了受領情報を決済管理手段およびクライアント手段に送信し，決済管理手段およびクライアントは，店舗手段から受信した第４署名の正当性を店舗手段の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【００５２】

店舗手段は，単一の店舗手段として構成しても良いし，複数の下層店舗手段を含むモールとして構成しても良い。

【００５３】

ここで，発明の理解を容易にするために，本発明に共通の用語について簡単に整理して説明する。

【００５４】

「電子決済システム」は，インターネットなどのオンライン通信系を介して商品やサービスの販売を行った場合に，代金決済を電子的にオンライン通信系を介して行うシステムである。オンライン通信系を介して決済を行う方法としては，クレジットカードやキャッシュカードやデビットカードによる支払い，プリペイドカードなどの電子マネーによる支払いが可能である。

【００５５】

「ＩＣカード」は，例えば，プラスチックなどのカードにＩＣチップが埋め込まれているものをいう。メモリチップのみを持っているタイプをメモリカードと呼び、ＣＰＵも搭載しているタイプはＣＰＵ内蔵カードと呼ばれる。さらに，ＩＣカードはＣＰＵの有無による種類のほかに、リーダライタに対する「接触」「非接触」でも区分できる。接触型は表面に金属の端子が載っていて、その端子を通してリーダライタと電力の供給やデータのやりとりを行う。それに対して、内部にアンテナを持ち、そのアンテナを通して電力供給やデータの読み取り／書き込みをするのが非接触型である。

【００５６】

「価値情報」は，ＩＣカードに記憶されて，商品やサービスの提供に対する対価として交換可能な価値に関する情報である。価値情報には，通貨に相当する貨幣的価値を有するものや，ポイントなどように商品やサービスと交換可能な擬似貨幣的価値を有するものが含まれる。

【００５７】

「クライアント装置」は，少なくともＩＣカードに対する情報入出力機能とインターネットなどのオンライン通信系を介して他の端末装置やサーバと双方向通信可能な機能を有する端末装置である。「クライアント装置」は，一般的には，演算装置，記憶装置，表示装置，入出力装置，通信装置，ＩＣカードリーダライタなどを備えたコンピュータ装置であり，同様の機能を有する携帯端末装置や携帯電話装置などを含む。クライアント装置の設置場所は，ユーザの家庭あるいは職場でも構わないし，あるいは本決済システム専用のクライアント端末が設置された店舗でも構わない。

【００５８】

「店舗装置」は，例えばインターネットなどのオンライン通信系を介して商品やサービスを販売等提供するネットワークサーバである。店舗装置は単一のネットワークサーバから構成しても，複数のネットワークサーバから構成されるモールとして構成しても構わない。

【００５９】

「決済管理装置」は，例えばＩＣカードと店舗装置間の決済を管理する管理サ

ーバであり，セキュリティサーバ，アプリケーションサーバ，データベースサーバなどから構成される。

【００６０】

「通信系」は，所定の通信プロトコルを介して双方向通信可能に構成された，例えば公衆回線網を利用したインターネットや，ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）やＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などのオンライン通信系であり，接続形態は有線無線を問わない。

【００６１】

「決済要求情報」は，店舗装置が作成するもので，ユーザがクライアント装置を介して店舗装置に送信した購買要求に対する決済を決済管理装置に要求するための各種情報が含まれる。この決済要求情報の正当性は，店舗装置の秘密鍵を用いて作成された第１署名を付し，決済管理装置がその第１署名を店舗装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【００６２】

「決済情報」は，決済管理装置が店舗装置から決済管理装置に送信された決済要求情報に基づいて作成するもので，決済管理装置からクライアント装置を介してＩＣカードに記憶された価値情報を増減することにより決済を行うための各種情報が含まれる。この決済情報のセキュリティは，決済管理装置とＩＣカードとの間で共用される共通鍵により確保される。さらに，決済情報の正当性は，決済管理装置の秘密鍵を用いて作成された第２署名を付し，クライアント装置がその第２署名を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【００６３】

「決済完了情報」は，決済管理装置がＩＣカードに記憶された価値情報を増減することにより決済が行われたことを確認した後に生成され，店舗装置に送信されるもので，決済完了に関する各種情報が含まれる。この決済完了情報の正当性は，決済管理装置の秘密鍵を用いて生成された第３署名を付し，店舗装置がその第３署名を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【００６４】

「決済完了受領情報」は，店舗装置がユーザが所有するＩＣカードに基づいて決済が完了したことを確認した後に生成されて，決済管理装置およびクライアント装置に送信されるもので，これにより決済の完了が確認され，店舗からユーザに対して商品またはサービスの受け渡しが可能となる。この決済完了情報の正当性は，店舗装置の秘密鍵を用いて生成された第４署名を付し，決済管理装置およびクライアント装置が店舗装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【００６５】

「価値更新情報」は，ＩＣカードに記憶されている価値情報を増減するための情報であり，決済管理装置からクライアント装置を介してＩＣカードに入力される。この価値更新情報のセキュリティは，決済管理装置とＩＣカードとの間で共用される共通鍵により確保される。さらに，価値更新情報の正当性は，決済管理装置の秘密鍵を用いて作成された第５署名を付し，クライアント装置がその第５署名を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【００６６】

「共通鍵」は，いわゆる共通鍵暗号化方式で，暗号化と復号化の双方に用いられる鍵であり，送り手と受け手が鍵を共用するものである。本発明においては，決済管理装置とＩＣカードとの間において共通鍵が設定される。

【００６７】

「秘密鍵」は，いわゆる公開鍵暗号化方式で暗号化に用いられる鍵であり，秘密鍵により暗号化された情報は，認証局などに保管されている対応する公開鍵により復号化が可能となる。

【００６８】

「公開鍵」は，いわゆる公開鍵暗号化方式で復号化に用いられる鍵であり，通常は，認証局になどに保管されており，受信者は，秘密鍵により暗号化された情報を復号化する際に，認証局から公開鍵を入手して復号化を行うものである。

【００６９】

「電子署名」は，送信される情報の正当性を保証するものであるが，送信側と受信側との種類に応じて，本発明においては第１署名～第５署名が使用される。

【００７０】

「第１署名」は，店舗装置の秘密鍵により作成され，決済要求情報に付されて，決済管理装置において，対応する公開鍵を用いて検証される署名である。

【００７１】

「第２署名」は，決済管理装置の秘密鍵により作成され，決済情報に付されて，クライアント装置において，対応する公開鍵を用いて検証される署名である。

【００７２】

「第３署名」は，決済管理装置の秘密鍵により作成され，決済完了情報に付されて，店舗装置において，対応する公開鍵を用いて検証される署名である。

【００７３】

「第４署名」は，店舗装置の秘密鍵により作成され，決済完了受領情報に付されて，決済管理装置において，対応する公開鍵を用いて検証される署名である。

【００７４】

「第５署名」は，決済管理装置の秘密鍵により作成され，価値更新求情報に付されて，クライアント装置において，対応する公開鍵を用いて検証される署名である。

【００７５】

【発明の実施の形態】　以下，添付図面を参照しながら，本発明の好適な実施形態にかかる電子決済システム，決済管理装置，店舗装置，クライアント装置，ＩＣカード，コンピュータプログラムおよび記憶媒体について説明する。

【００７６】

図１は，本実施形態にかかる電子決済システムを適用可能な電子決済システム１の全体構成図である。

【００７７】

図１に示すように，電子決済システム１は，クライアント装置およびＩＣカードを含むユーザ２，決済管理装置３および店舗装置４の間で，所定の通信プロトコルを介して双方向通信可能な通信系であるインターネットなどのネットワーク

５を介した通信を行うことが可能である。

【００７８】

〔ユーザ２〕

ユーザ２には，ＩＣカード２０と，ＩＣカード２０にアクセスして情報の入出力を行うリーダライタ装置２１およびパーソナルコンピュータ２２などから構成されるクライアント装置が設けられている。

【００７９】

ＩＣカード２０は，例えば，プラスチックなどのカードにＩＣチップが埋め込まれているものである。ＩＣカード２０は，図２（Ａ）に示すように耐タンパ性のＩＣモジュール５０を有し，図２（Ｂ）に示すように当該ＩＣモジュール５０内に処理回路５１およびメモリ５２を内蔵している。

【００８０】

ＩＣカード２０の処理回路５１は，決済管理装置３のセキュリティサーバ３１との間で共用される共通鍵ＫＣを用いた復号処理，所定の情報および要求に応じた処理，並びに相互認証処理などの種々の処理を行うことが可能である。

【００８１】

メモリ５２は，決済管理装置３のセキュリティサーバ３１との間で共用する共通鍵ＫＣを記憶している。

【００８２】

ＩＣカード２０は，図３に示すように，ＩＣカードリーダライタ２１を介してパーソナルコンピュータ２２と通信を行い，パーソナルコンピュータ２２内で駆動するＡｃｔｉｖｅＸコンポーネントなどのインタフェースプログラム２４やブラウザプログラム２３を介して，インターネットなどのネットワーク５に接続する。さらに，ＩＣカード２０は，決済管理装置３のアプリケーションサーバ３０を介して，セキュリティサーバ３１に接続し，セキュリティサーバ３１との間で情報を送受信する。このように確立されるＩＣカード２０とセキュリティサーバ３１との間の情報通信は，共通鍵ＫＣを用いた共通鍵暗号化方式（ＰＫＩプロトコル）によって暗号化および復号化されることにより，セキュリティが確保されている。

【００８３】

なお，ＩＣカードには，価値情報が記憶されている。この価値情報は，商品やサービスの提供に対する対価として交換可能な価値に関する情報である。価値情報には，通貨に相当する貨幣的価値を有するものや，ポイントなどように商品やサービスと交換可能な擬似貨幣的価値を有するものが含まれる。

【００８４】

ＩＣカードのリーダライタ２１は，ＩＣカード２０のＩＣモジュール５０との間で非接触方式あるいは接触方式でデータ入出力を行うと共に，パーソナルコンピュータ２２との間との間で情報および要求の入出力を行うものである。

【００８５】

パーソナルコンピュータ２２は，ユーザによるキーボードやマウスなどの操作に応じて，ブラウザプログラム２３を実行すると共に，ブラウザプログラム２３上で，後述するようにネットワーク５を介して決済管理装置３のアプリケーションサーバ３０から受信したＡｃｔｉｖｅＸコンポーネントなどのインタフェースプログラム２４を実行する。

【００８６】

パーソナルコンピュータ２２は，ディスプレイ，キーボードおよびマウスなどを有している。なお，図示の例では，クライアント装置の例として，リーダライタ２１が接続可能なパーソナルコンピュータ２２を挙げているが，ＩＣカードとの間で接触または非接触に情報交換を行うことが可能な機器であれば，パーソナルコンピュータ２２に限定されず，携帯端末装置や携帯電話端末装置などを使用することも可能である。

【００８７】

ブラウザプログラム２３は，図４に示すように，例えば，マイクロソフト社のインターネットエクスプローラーなどのようにパーソナルコンピュータ２２上で動作して，ネットワークサーバが提供するサービスをクライアント側の端末上で表示させることが可能なプログラムである。本実施の形態においては，ブラウザプログラム２３は，店舗装置４のネットワークサーバ４０のＨＴＴＰＳレイヤ６０との間で，ＰＫＩプロトコルにより，送信元において自らの秘密鍵を用いた署

名情報の付加，並びに送信先において当該秘密鍵に対応する公開鍵を用いた当該署名情報の検証を行う。

【００８８】

インタフェースプログラム２４は，図５に示すように，パーソナルコンピュータ２２上で動作し，決済管理装置３のアプリケーションサーバ３０のＡＰＳ上位レイヤ３０ａとの間で，ＰＫＩプロトコルにより，送信元において自らの秘密鍵を用いた署名情報の付加，並びに送信先において当該秘密鍵に対応する公開鍵を用いた当該署名情報の検証を行うことが可能なプログラムである。

【００８９】

また，インタフェースプログラム２４は，ブラウザプログラム２３を実行中に，リーダライタ２１を介してＩＣカード２０などのローカル資源へのアクセスを容易に実現するための機能拡張プログラムとしても機能する。

【００９０】

〔決済管理装置３〕

決済管理装置３には，図１および図６に示すように，バーチャル電子マネーシステムとして機能するアプリケーションサーバ３０，セキュリティ管理システムとして機能するセキュリティサーバ３１，精査・決済システムとして機能する情報管理サーバ３２，さらに本実施の形態とは直接的な関係はないが，リアル電子マネーシステムとして機能するアプリケーションサーバ３３が設けられている。

【００９１】

決済管理装置３のアプリケーションサーバ３０は，インターネットなどのネットワーク５を介して，ユーザ２のパーソナルコンピュータ２２や店舗装置４のネットワークサーバ４０と双方向通信が可能である。

【００９２】

また，決済管理装置３のアプリケーションサーバ３０は，店舗装置４のネットワークサーバ４０の秘密鍵ＫSHOP,Sに対応した公開鍵ＫSHOP,Pを保持し，後述するように，店舗装置４のネットワークサーバ４０が生成した決済要求情報ＢＩＬＬに付された第１署名情報ＳＩＧ１を検証する。

【００９３】

さらに，決済管理装置３のアプリケーションサーバ３０は，図５に示すように，ＡＰＳ上位レイヤ３０ａおよびＡＰＳ下位レイヤ３０ｂを有する。

【００９４】

決済管理装置３のセキュリティサーバ３１は，ユーザ２のＩＣカード２０との間で共用する共通鍵ＫＣを記憶している。

【００９５】

決済管理装置３のセキュリティサーバ３１は，図５に示すように，ＩＣカードのリーダライタ２１，インタフェースプログラム２４，ブラウザプログラム２３，パーソナルコンピュータ２２，ネットワーク５およびアプリケーションサーバ３０を介して，ＩＣカード２０との間で送受信する情報を，共通鍵ＫＣを用いた共通鍵暗号方式によって暗号化および復号する。

【００９６】

情報管理サーバ３２は，例えば，登録されたユーザの個人情報を記憶および管理する。

【００９７】

〔店舗装置４〕

店舗装置４には，ネットワークサーバ４０が設けられている。

【００９８】

店舗装置４のネットワークサーバ４０は，図４に示すように，パーソナルコンピュータ２２上で動作するブラウザプログラム２３とＨＴＴＰＳレイヤの間で，ＰＫＩプロトコルを介して双方向通信することが可能なように構成されている。

【００９９】

また，店舗装置４のネットワークサーバ４０は，例えば，商品あるいはサービスの紹介情報を記憶すると共に，店舗装置４がユーザ２に請求する金額に対応する決済を要求する決済要求情報ＢＩＬＬと，当該決済要求情報に対して自らの秘密鍵ＫSHOP,Sを用いて作成した第１署名情報ＳＩＧとを生成する。

【０１００】

店舗装置４は，図６に示すように単一の加盟店４２として構成することが可能である。あるいは，店舗装置４は，図６に示すように，モール４１の加盟店とし

て構成される加盟店４２として構成することも可能である。

【０１０１】

なお，図６に示す電子決済システムの構成例においては，ユーザがパーソナルコンピュータ２２などを介してバーチャルにショッピングを行う際の決済に適用されるバーチャル電子マネーシステム３０に加えて，ユーザが実際に店舗７に出かけてリアルにショッピングを行う際の決済に適用されるリアル電子マネーシステム３３も含んでいる。

【０１０２】

リアル電子マネーシステム３３に対しては，公衆回線網６などの通信系を介して，ユーザが実際に訪問可能なリアル店舗７が接続されている。リアル店舗７は，独立店舗７１として構成することも可能であり，あるいは本部７２に従属する従属店舗７２として構成することも可能である。ただし，リアル電子マネーシステム３３については，本発明の要旨とは異なるので詳細説明は省略する。

【０１０３】

次に図７を参照しながら，本実施の形態にかかる決済システムにおける情報の流れについて説明する。

【０１０４】

すでに説明したように，本実施の形態にかかる決済システムにおいては，情報の受け手および送り手は，決済管理装置３，店舗装置４，パーソナルコンピュータ２２およびリーダライタ２１から成るクライアント装置２およびＩＣカード２０である。

【０１０５】

上記情報の受け手および送り手間において流通する情報は，購買要求情報，決済要求情報，決済情報，決済完了情報，決済完了受領情報，価値更新情報などがある。

【０１０６】

「購買要求情報」は，ユーザがクライアント装置であるパーソナルコンピュータ２２のブラウザ２３を介して店舗装置４のネットワークサーバ４０にアクセスし，店舗装置４のサイトが展開する商品やサービスの中から，購入したい商品ま

たはサービスを選択し，店舗装置４に送信する情報である。

【０１０７】

「決済要求情報」は，店舗装置４が作成するもので，ユーザがクライアント装置であるパーソナルコンピュータ２２を介して店舗装置に送信した購買要求情報に対する決済を決済管理装置３に要求するための各種情報が含まれる。この決済要求情報の正当性は，店舗装置４の秘密鍵を用いて作成された第１署名を付し，決済管理装置３がその第１署名を店舗装置４の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【０１０８】

「決済情報」は，決済管理装置３が店舗装置４から決済管理装置３に送信された決済要求情報に基づいて作成するもので，決済管理装置３からクライアント装置であるパーソナルコンピュータ２２およびリーダライタ２１を介してＩＣカード２０に記憶された価値情報を増減することにより決済を行うための各種情報が含まれる。この決済情報のセキュリティは，決済管理装置３とＩＣカード２０との間で共用される共通鍵により確保される。さらに，決済情報の正当性は，決済管理装置３の秘密鍵を用いて作成された第２署名を付し，クライアント装置であるパーソナルコンピュータ２２がその第２署名を決済管理装置３の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【０１０９】

「決済完了情報」は，決済管理装置３がＩＣカード２０に記憶された価値情報を増減することにより決済が行われたことを確認した後に生成され，店舗装置４に送信されるもので，決済完了に関する各種情報が含まれる。この決済完了情報の正当性は，決済管理装置３の秘密鍵を用いて生成された第３署名を付し，店舗装置４がその第３署名を決済管理装置３の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【０１１０】

「決済完了受領情報」は，店舗装置４がユーザが所有するＩＣカード２０に基づいて決済が完了したことを確認した後に生成されて，決済管理装置３およびクライアント装置であるパーソナルコンピュータ２２に送信されるもので，これに

より決済の完了が確認され，店舗装置４からユーザに対して商品またはサービスの受け渡しが可能となる。この決済完了情報の正当性は，店舗装置４の秘密鍵を用いて生成された第４署名を付し，決済管理装置３およびクライアント装置であるパーソナルコンピュータ２２が店舗装置４の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【０１１１】

「価値更新情報」は，ＩＣカード２０に記憶されている価値情報を増減するための情報であり，決済管理装置３からクライアント装置であるパーソナルコンピュータ２２およびリーダライタ２１を介してＩＣカード２０に入力される。この価値更新情報のセキュリティは，決済管理装置３とＩＣカード２０との間で共用される共通鍵により確保される。さらに，価値更新情報の正当性は，決済管理装置３の秘密鍵を用いて作成された第５署名を付し，クライアント装置であるパーソナルコンピュータ２２がその第５署名を決済管理装置３の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【０１１２】

なお，本実施の形態にかかる決済システムにおいて，送信される情報の正当性を保証するために用いられる電子署名は，送信側と受信側との種類に応じて，第１署名～第５署名が使用される。

【０１１３】

「第１署名」は，店舗装置４の秘密鍵により作成され，決済要求情報に付されて，決済管理装置３において，対応する公開鍵を用いて検証される署名である。

【０１１４】

「第２署名」は，決済管理装置３の秘密鍵により作成され，決済情報に付されて，クライアント装置であるパーソナルコンピュータ２２において，対応する公開鍵を用いて検証される署名である。

【０１１５】

「第３署名」は，決済管理装置３の秘密鍵により作成され，決済完了情報に付されて，店舗装置４において，対応する公開鍵を用いて検証される署名である。

【０１１６】

「第４署名」は，店舗装置４の秘密鍵により作成され，決済完了受領情報に付されて，決済管理装置３において，対応する公開鍵を用いて検証される署名である。

【０１１７】

「第５署名」は，決済管理装置３の秘密鍵により作成され，価値更新求情報に付されて，クライアント装置であるパーソナルコンピュータ２２において，対応する公開鍵を用いて検証される署名である。

【０１１８】

次に，図８を参照しながら，本実施の形態にかかる決済システムにおける電子マネー出金動作について説明する。

【０１１９】

ユーザ２は，パーソナルコンピュータ２２を介して加盟店４２の根とワークサーバ４０にアクセスし，サイトにおいて提供される商品またはサービスの中から，ユーザ２が購入を希望する商品またはサービスの選択を行う（①）。

【０１２０】

加盟店４２は，ユーザ２が選択した商品またはサービスの合計金額に関する情報をユーザに送信する（②）。

【０１２１】

ユーザ２は，加盟店４２が所属するモール４１に対して，本実施の形態にかかる決済システムを利用し電子マネーによる決済を依頼する（③）。

【０１２２】

ユーザ２からの電子マネー決済依頼を受けて，モール４１は，受注番号を発番するとともに，第１署名付決済要求情報を発行する（④）。

【０１２３】

ユーザ２はモール４１から送信された第１署名付決済要求情報およびカード情報（ＩＤ，残高等）をサイバー電子マネーシステム３０に送信する（⑤）。

【０１２４】

サイバー電子マネーシステム３０は，第１署名付決済要求情報を受けて，ユーザ２が所有するＩＣカード２０と通信を行い，第２署名付決済情報をＩＣカード

２０に送信し，ＩＣカード２０内に記憶されている価値情報から購入する商品またはサービスに対応する価値を減算し，カード内の履歴情報を吸い上げる（⑥）。

【０１２５】

サイバー電子マネーシステム３０は，決済が完了した後に，第３署名付決済完了情報をモール７１に送信する（⑦）。

【０１２６】

サイバー電子マネーシステム３０は，決済が完了した後に，第３署名付決済完了情報をユーザ２に送信する（⑧）。

【０１２７】

第３署名付決済完了情報により決済が完了したことを確認した後に，ユーザ２は加盟店４２に対して決済完了画面を要求する（⑨）。

【０１２８】

加盟店４は，ユーザ２からの決済完了画面要求に応じて，第４署名付決済完了受領情報をユーザ２およびサイバー電子マネーシステム３０に送信するとともに，決済完了画面をユーザ２のパーソナルコンピュータ２２に表示する（10）。

【０１２９】

以上の工程により決済が完了した後に，加盟店４２からユーザ２に対して商品またはサービスが受け渡される。例えば，商品がデジタルコンテンツであるような場合には，加盟店４２がユーザ２に対して，デジタルコンテンツのダウンロードを許可することにより，商品の受け渡しが行われる（11）。

【０１３０】

次に，図９～図１１を参照しながら，共通鍵，公開鍵，および電子署名を用いた請求リティの高い本実施の形態にかかる電子決済システムおける商品情報伝送シーケンスおよび価値情報伝送シーケンスについて，詳細に説明する。

【０１３１】

まず，図９示すユーザによる商品決定が行われる前に，ユーザ２がパーソナルコンピュータ２２上で動作するブラウザプログラム２３を用いて，ネットワーク５を介して，店舗装置４のネットワークサーバ４０にアクセスを行う。当該アク

セスにより，ネットワーク５を介してネットワークサーバ４０からパーソナルコンピュータ２２に，店舗装置４が提供する商品情報が送信され，それに応じた画面がパーソナルコンピュータ２２のディスプレイに表示される。

【０１３２】

（第１実施形態）　以下，電子決済システム１の動作を図９～図１１各ステップ毎に説明する。なお，図１２～図２０には，クライアント装置のパーソナルコンピュータ２２の画面表示される例が示されている。

【０１３３】

なお，以下に示す動作において，クライアント装置のパーソナルコンピュータ２２とネットワークサーバ４０との間で情報あるいは要求の送受信を行う際に，送信元の秘密鍵を用いて作成した署名情報を，送信先において，当該秘密鍵に対応する公開鍵を用いて検証するが，当該処理については記載を省略する。

【０１３４】

また，同様に，パーソナルコンピュータ２２とアプリケーションサーバ３０との間で情報あるいは要求の送受信を行う際に，送信元の秘密鍵を用いて作成した電子署名情報を，送信先において，当該秘密鍵に対応する公開鍵を用いて検証するが，当該処理についてはステップＳＴ１４，ＳＴ１５を除いて記載を省略する。

【０１３５】

ステップＳＴ１：

パーソナルコンピュータ２２とネットワークサーバ４０との間でＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）を用いた相互認証を行い，セキュアな通信路を確立する。

【０１３６】

ステップＳＴ２：

ユーザ２が，図１２に示すような商品選択画面において，パーソナルコンピュータ２２のキーボードやマウスなどを操作して購入を希望する商品を決定すると，それに応じた商品決定情報がパーソナルコンピュータ２２からネットワークサーバ４０に送信される。

【０１３７】

ステップＳＴ３：

ネットワークサーバ４０は，パーソナルコンピュータ２２から商品決定情報を受けると，その見積もり情報をパーソナルコンピュータ２２に送信する。

【０１３８】

ステップＳＴ４：

パーソナルコンピュータ２２は，図１３に示すように，ネットワークサーバ４０から受けた見積もり情報をディスプレイに表示する。ユーザ２は，当該見積もりに同意した場合には，図１４に示す画面において，支払い方法を選択する。ユーザ２が，パーソナルコンピュータ２２のキーボードなどを操作して電子マネーを利用した決済を選択すると，請求額要求がネットワークサーバ４０に送信される。

【０１３９】

ステップＳＴ５：

ネットワークサーバ４０は，パーソナルコンピュータ２２から請求額要求を受けると，店舗装置４がユーザ２に請求する金額を示す決済要求情報と，当該決済要求情報に対して店舗装置４の秘密鍵KSHOP,Sを用いて作成した第１署名情報ＳＩＧ１と，インタフェースプログラム２４とをパーソナルコンピュータ２２に送信する。

【０１４０】

ステップＳＴ６：

パーソナルコンピュータ２２は，図１５に示すように，ステップＳＴ５でネットワークサーバ４０から受信した決済要求情報が示す金額をディスプレイに表示する。

【０１４１】

ステップＳＴ７：

ステップＳＴ６でディスプレイに表示された金額に同意したユーザ２がパーソナルコンピュータ２２のキーボードなどを用いて所定の指示を出すと，ステップＳＴ５でネットワークサーバ４０から受信したインタフェースプログラム２４が

起動される。

【０１４２】

そして，図１６に示すような画面表示にしたがって，ユーザ２がＩＣカード２０をリーダライタ２１にかざすと，パーソナルコンピュータ２２は，起動されたインタフェースプログラム２４を用いて，決済管理装置３のアプリケーションサーバ３０との間でＳＳＬを用いた相互認証を行い，セキュアな通信路を確立する。

【０１４３】

本実施の形態にかかる決済システムにおいて決済処理が行われている間は，パーソナルコンピュータ２２のディスプレイには，図１７に示すように，ユーザに待機を促すような画面が表示される。

【０１４４】

ステップＳＴ８：

パーソナルコンピュータ２２は，ステップＳＴ５で店舗装置４のネットワークサーバ４０から受信した決済要求情報と，当該決済要求情報に対する第１署名情報ＳＩＧ１とを含む決済要求情報を決済管理装置３のアプリケーションサーバ３０に送信する。

【０１４５】

ステップＳＴ９：

アプリケーションサーバ３０は，例えば，情報管理サーバ３２から読み出した店舗装置４に対応する公開鍵KSHOP,Pを用いて，ステップＳＴ８で受信した第１署名情報ＳＩＧ１を検証し，当該第１署名情報ＳＩＧ１が店舗装置４のネットワークサーバ４０において付された正当なものであると判断すると，ステップＳＴ１０の処理を行う。

【０１４６】

なお，アプリケーションサーバ３０は，第１署名情報ＳＩＧ１が不正なものであると判断した場合には，例えば，パーソナルコンピュータ２２に対してのその旨を通知した後，処理を終了する。

【０１４７】

ステップＳＴ１０：

次いで，決済管理装置３のアプリケーションサーバ３０は，例えば，決済要求情報をセキュリティサーバ３１に送信する。

【０１４８】

ステップＳＴ１１：

セキュリティサーバ３１は，ＩＣカード２０から決済要求情報を受けると，ＩＣカード２０との間で相互認証を行い，ＩＣカード２０との間で用いる共通鍵ＫＣからセッション鍵ＫSESを生成する。ＩＣカード２０でも，同様に，共通鍵ＫＣからセッション鍵ＫSESを生成する。

【０１４９】

ステップＳＴ１２：

セキュリティサーバ３１は，決済情報を生成し，これをセッション鍵ＫSESで暗号化してアプリケーションサーバ３０に出力する。その際に，セキュリティサーバ３１は，決済管理装置の秘密鍵を用いて作成した第２署名を付す。

【０１５０】

アプリケーションサーバ３０は，セキュリティサーバ３１から入力した残高読み出し要求（ＢＲＣ）を含む決済情報をパーソナルコンピュータ２２に送信する。

【０１５１】

パーソナルコンピュータ２２は，アプリケーションサーバ３０から受信した残高読み出し要求ＢＲＣを含む決済情報をリーダライタ２１を介してＩＣカード２０に出力する。

【０１５２】

ステップＳＴ１３：

ＩＣカード２０は，パーソナルコンピュータ２２からの残高読み出し要求ＢＲＣを含む決済情報が入力されると，これをステップＳＴ１１で生成したセッション鍵ＫSESを用いて復号する。

【０１５３】

そして，ＩＣカード２０は，残高読み出し要求ＢＲＣを含む決済情報に応じた

処理回路５１の処理によって，ＩＣカード２０内の耐タンパ性のメモリ５２から残高情報ＢＩを含む決済情報を読み出し，これをセッション鍵KSESを用いて暗号化した後に，パーソナルコンピュータ２２に出力する。

【０１５４】

パーソナルコンピュータ２２は，ＩＣカード２０からの残高情報ＢＩを含む決済情報をアプリケーションサーバ３０に送信する。

【０１５５】

アプリケーションサーバ３０は，パーソナルコンピュータ２２から受信した残高情報ＢＩを決済情報をセキュリティサーバ３１に出力する。

【０１５６】

セキュリティサーバ３１は，アプリケーションサーバ３０から入力した残高情報ＢＩを含む決済情報をセッション鍵KSESを用いて復号し，ログ情報を生成する。

【０１５７】

ステップＳＴ１４：

セキュリティサーバ３１は，ステップＳＴ１３で生成したログ情報をＩＣカード２０に書き込むためのログ書き込み情報と，ＩＣカード２０に記憶された残高情報が示す金額から請求額を減算するための減算額を示す減算情報とを含む決済処理要求ＳＰＣを生成し，これをセッション鍵KSESを用て暗号化する。

【０１５８】

次に，セキュリティサーバ３１は，平文の残高情報ＢＩと，暗号化された決済処理要求ＳＰＣとを含む決済情報をアプリケーションサーバ３０に出力する。

【０１５９】

アプリケーションサーバ３０は，セキュリティサーバ３１から入力した残高情報ＢＩおよび決済処理要求ＳＰＣを含む決済情報に対する第２署名情報をアプリケーションサーバ３０の秘密鍵を用いて作成する。

【０１６０】

次に，アプリケーションサーバ３０は，セキュリティサーバ３１から入力した残高情報ＢＩおよび決済処理要求ＳＰＣを含む決済情報に対して第２署名情報を

付してパーソナルコンピュータ２２に送信する。

【０１６１】

ステップＳＴ１５：

パーソナルコンピュータ２２は，アプリケーションサーバ３０から受信した第２署名情報ＳＩＧ２の正当性を，アプリケーションサーバ３０の公開鍵を用いて検証し，その正当性が認められた後に，以下に示す処理を行う。

【０１６２】

パーソナルコンピュータ２２は，図１８に示すように，アプリケーションサーバ３０から受信した残高情報ＢＩが示す残高，並びにステップＳＴ３でネットワークサーバ４０から受信した見積もり情報が示す金額（請求額）をディスプレイに表示する。

【０１６３】

ステップＳＴ１６：

パーソナルコンピュータ２２は，ステップＳＴ１５でディスプレイに表示された残高および請求額に同意したユーザ２がパーソナルコンピュータ２２のキーボードなどを用いて所定の指示を出すと，決済処理要求ＳＰＣをＩＣカードリーダライタ２１を介してＩＣカード２０に出力する。支払確認処理が行われている間は，図１９に示すような待機を促す画面がパーソナルコンピュータ２２のディスプレイに表示される。

【０１６４】

ステップＳＴ１７：

ＩＣカード２０は，パーソナルコンピュータ２２から入力した決済処理要求ＳＰＣをセッション鍵KSESを用いて復号し，当該決済処理要求に応じた決済処理を処理回路５１で実行する。

【０１６５】

具体的には，ＩＣカード２０は，処理回路５１の処理によって，決済処理要求ＳＰＣに含まれるログ書き込み情報を，ＩＣカード２０内の耐タンパ性のメモリ５２に記憶する。また，ＩＣカード２０は，処理回路５１の処理によって，メモリ５２に記憶されている残高情報が示す残高から，決済処理要求ＳＰＣに含まれ

る減算情報が示す減算額を減算し，その結果を残高情報としてメモリ５２に記憶する。

【０１６６】

ステップＳＴ１８：

ＩＣカード２０は，ステップＳＴ１７の処理が完了すると，処理が完了したことを示す処理完了通知ＰＣＮを生成し，これをセッション鍵ＫSESで暗号化した後に，パーソナルコンピュータ２２およびアプリケーションサーバ３０を介して，セキュリティサーバ３１に送信する。

【０１６７】

ステップＳＴ１９：

セキュリティサーバ３１は，ＩＣカード２０からの処理完了通知ＰＣＮを受信すると，これをセッション鍵ＫSESを用いて復号し，処理完了通知ＰＣＮを確認した後に，決済完了情報ＡＣＮを生成し，これをアプリケーションサーバ３０を介してパーソナルコンピュータ２２およびネットワークサーバ４０に送信する。その際に，決済完了情報は，決済管理装置が生成する第３署名を付することにより，その正当性が確保される。

【０１６８】

ステップＳＴ２０：

パーソナルコンピュータ２２は，セキュリティサーバ３１からの決済完了通知ＡＣＮを受信すると，図２０に示すように，これに応じた情報，例えばデジタルコンテンツのダウンロードを促すような画面をディスプレイに表示する。

【０１６９】

以上説明したように，電子決済システム１によれば，ＩＣカード２０のメモリ５２に共通鍵ＫCを記憶し，秘密鍵は記憶しない。そのため，ユーザ２がＩＣカード２０を紛失した場合でも，メモリ５２には秘密鍵が記憶されていないため，秘密鍵を用いてユーザ２の署名が不正に行われることを回避できる。

【０１７０】

また，電子決済システム１によれば，共通鍵ＫCはＩＣカード２０およびセキュリティサーバ３１の内部でのみ使用されることから，共通鍵ＫCが盗まれる危

険性を低くでき，安全な取り引きを実現できると共に，鍵管理を容易にすることができる。

【０１７１】

また，電子決済システム１によれば，ＩＣカード２０に入出力される情報および要求をパーソナルコンピュータ２２を介して行い，パーソナルコンピュータ２２と，アプリケーションサーバ３０およびネットワークサーバ４０との間で情報および要求を送受信する際に，秘密鍵および公開鍵を用いた署名検証を行うことから，当該情報および要求がネットワーク５上で不正に改竄されることを回避でき，ネットワーク５を用いた取り引きの安全性を確保できる。

【０１７２】

また，電子決済システム１によれば，店舗装置４のネットワークサーバ４０において，請求額情報ＢＩＬＬに対して自らの秘密鍵ＫSHOP,Sを用いて作成した署名情報ＳＩＧを付し，決済管理装置３のアプリケーションサーバ３０において，秘密鍵ＫSHOP,Sに対応する公開鍵ＫSHOP,Pを用いて署名情報ＳＩＧを検証し，当該署名情報ＳＩＧが店舗装置４のネットワークサーバ４０において付された正当なものであると判断することから，ユーザ２のパーソナルコンピュータ２２などにおいて，不正に改竄された請求額情報ＢＩＬＬに基づいて決済が行われてしまうことを防止できる。

【０１７３】

また，電子決済システム１では，前述したように，パーソナルコンピュータ２２は，アプリケーションサーバ３０から受信した残高情報ＢＩが示す残高，並びにネットワークサーバ４０から受信した見積もり情報が示す金額（請求額）をディスプレイに表示し，その内容にユーザ２が同意した後に，アプリケーションサーバ３０から受信した決済処理要求ＳＰＣをＩＣカードリーダライタ２１を介してＩＣカード２０に出力する。従って，ユーザ２は，ＩＣカード２０内で最終的に行われる決済処理の内容を事前に確認でき，不正に改竄された内容で決済処理が行われることを防止できる。

【０１７４】

また，電子決済システム１によれば，決済処理に伴う手順を従来に比べて少な

くでき，ネットワーク５を介した情報伝送を削減でき，ネットワーク５の利用量の削減，並びに処理時間を短縮を図れる。

【０１７５】

また，電子決済システム１によれば，従来のＳＥＴ方式のように，署名情報の作成および検証を多数回行う必要がない。

【０１７６】

（第２実施形態）

次に図２１～図２３を参照しながら，別の実施の形態にかかる決済システムによる商品情報伝送シーケンスおよび価値情報伝送シーケンスについて説明する。

【０１７７】

ＳＴ１０１：

まず，ユーザ２のパーソナルコンピュータ２２と店舗装置４のネットワークサーバ４０との間においてセキュリティにすぐれた通信のためにＳＳＬ認証が確立される。

【０１７８】

ＳＴ１０２：

次いで，ユーザ２は，パーソナルコンピュータ２２のディスプレイに表示される画面に応じて，商品の選択を行う。

【０１７９】

ＳＴ１０３：

店舗装置４のネットワークサーバ４０は，ユーザ２が選択した商品に応じて，店舗装置４の秘密鍵を用いて作成された第１署名が付された決済処理要求情報を，ユーザ２のパーソナルコンピュータ２２に送信する。

【０１８０】

ＳＴ１０４：

パーソナルコンピュータ２２は，ＡｃｔｉｖｅＸなどのインタフェースプログラム２４を起動して，リーダライタ２１を介してＩＣカード２０にアクセスし，ＩＣカードの残高を読み出す。

【０１８１】

ＳＴ１０５：

読み出された残高は，所定のブラウジング機構を利用して，ユーザ２のパーソナルコンピュータ２２に取り込まれ，ディスプレイ上に表示される。

【０１８２】

ＳＴ１０６：

次いで，ユーザ２のパーソナルコンピュータ２２と決済管理装置３のアプリケーションサーバ３０との間にセキュアなＳＳＬ認証を確立し，価値情報伝送シーケンスに備える。

【０１８３】

ＳＴ１０７：

次いで，ユーザ２のパーソナルコンピュータ２２からＩＣカード２０の残高情報を含む第１署名付の決済要求情報が決済管理装置３に送信される。

【０１８４】

決済管理装置３のアプリケーションサーバ３０は，店舗装置４の秘密鍵に対応する公開鍵により，送信された決済要求情報の正当性を検証し，必要な情報をセキュリティサーバ３１に受け渡す。

【０１８５】

ＳＴ１０８：

決済管理装置３のセキュリティサーバ３１は，ＩＣカード２０との間で相互認証を行い，共通鍵からセッション鍵を生成する。同様に，ＩＣカード２０側においても，セキュリティサーバ３１との間で相互認証を行い，共通鍵からセッション鍵を生成する。

【０１８６】

ＳＴ１０９：

セキュリティサーバ３１は，決済情報をセッション鍵で暗号化し，アプリケーションサーバ３０を介してユーザ２のパーソナルコンピュータ２２に送信する。

【０１８７】

パーソナルコンピュータ２２では，送られてきた決済情報を，ＩＣカード２０が記憶しているセッション鍵で復号化して画面表示する。ユーザ２が送られてき

た決済情報を承認する場合には，リーダライタ２１を介して，その内容がＩＣカード２０に送信され，ＩＣカード２０内において，減算処理などの所定の決算処理が行われる。

【０１８８】

なお，ここで留意すべきは，本実施形態にかかる決算シーケンスにおいては，図９～図１１に関連して説明した決算シーケンスとは異なり，決算管理装置３のセキュリティサーバ３１により生成される決算情報は，単に共通鍵により暗号化されるのみで，決算管理装置３が有する秘密鍵を用いて生成される第２署名が付されない点である。

【０１８９】

このように，単に共通鍵による暗号化／復号化によっても，送信される決算情報の身元は確認可能なので，本実施の形態にかかる決算システムのように，第２署名を省略することにより，処理の冗長性を緩和することが可能である。

【０１９０】

ＳＴ１１０：

以上説明したようにして，ＩＣカード２０内において，所定の決算処理が終了すると，その結果が，リーダライタ２１，パーソナルコンピュータ２２，アプリケーションサーバ３０を介してセキュリティサーバ３１に送信される。

【０１９１】

ＳＴ１１１：

セキュリティサーバ３１により決算完了が確認されると，その決算完了情報がアプリケーションサーバ３０に送られる。そして，決算完了情報（領収書）は，アプリケーションサーバ３１において，決算管理装置３の秘密鍵を用いて生成された第３署名が付されて，店舗装置２のネットワークサーバ４０に送信される。

【０１９２】

ＳＴ１１２：

ネットワークサーバ４０においては，決算管理装置３の秘密鍵に対応する公開鍵により決算完了情報を検証し，その内容を確認後，決済完了受領情報を生成する。この決済完了受領情報は，店舗装置４の秘密鍵を用いて生成された第４署名

が付されて，決算管理装置３のアプリケーションサーバ３０に送信される。

【０１９３】

そして，決算管理装置３のアプリケーションサーバ３０が，第４署名付決済完了受領情報を，ユーザ２のパーソナルコンピュータ２２に送信することにより，パーソナルコンピュータ２２のディスプレイには，一連の電子マネー決算処理が完了した旨の表示が成される。

【０１９４】

以上説明したように，本実施の形態にかかる電子決済システムによれば，ＩＣカード２０のメモリ５２に共通鍵を記憶し，秘密鍵は記憶しない。そのため，ユーザ２がＩＣカード２０を紛失した場合でも，メモリ５２には秘密鍵が記憶されていないため，秘密鍵を用いてユーザ２の署名が不正に行われることを回避できる。

【０１９５】

また，本実施の形態にかかる電子決済システムによれば，共通鍵はＩＣカード２０およびセキュリティサーバ３１の内部でのみ使用されることから，共通鍵が盗まれる危険性を低くでき，安全な取り引きを実現できると共に，鍵管理を容易にすることができる。

【０１９６】

また，本実施の形態にかかる電子決済システムによれば，ＩＣカード２０に入出力される情報および要求をパーソナルコンピュータ２２を介して行い，パーソナルコンピュータ２２と，アプリケーションサーバ３０およびネットワークサーバ４０との間で情報および要求を送受信する際に，秘密鍵および公開鍵を用いた署名検証を行うことから，当該情報および要求がネットワーク５上で不正に改竄されることを回避でき，ネットワーク５を用いた取り引きの安全性を確保できる。

【０１９７】

なお署名検証を行わない場合であっても，共通鍵による暗号化／復号化によって，送信される決算情報の身元は確認可能なので，本実施の形態にかかる決算システムのように，処理の冗長性を緩和することが可能である。

【０１９８】

また，本実施の形態にかかる電子決済システムによれば，店舗装置４のネットワークサーバ４０において，決済要求情報に対して自らの秘密鍵を用いて作成した第１署名情報を付し，決済管理装置３のアプリケーションサーバ３０において，秘密鍵に対応する公開鍵を用いて第１署名情報を検証し，当該第１署名情報が店舗装置４のネットワークサーバ４０において付された正当なものであると判断することから，ユーザ２のパーソナルコンピュータ２２などにおいて，不正に改竄された決済要求情報に基づいて決済が行われてしまうことを防止できる。

【０１９９】

また，本実施の形態にかかる電子決済システムでは，前述したように，パーソナルコンピュータ２２は，アプリケーションサーバ３０から受信した残高情報が示す残高，並びにネットワークサーバ４０から受信した見積もり情報が示す金額（請求額）をディスプレイに表示し，その内容にユーザ２が同意した後に，アプリケーションサーバ３０から受信した決済処理要求ＳＰＣをＩＣカードリーダライタ２１を介してＩＣカード２０に出力する。従って，ユーザ２は，ＩＣカード２０内で最終的に行われる決済処理の内容を事前に確認でき，不正に改竄された内容で決済処理が行われることを防止できる。

【０２００】

また，電子決済システム１によれば，決済処理に伴う手順を従来に比べて少なくでき，ネットワーク５を介した情報伝送を削減でき，ネットワーク５の利用量の削減，並びに処理時間を短縮を図れる。

【０２０１】

また，電子決済システム１によれば，従来のＳＥＴ方式のように，署名情報の作成および検証を多数回行う必要がないがないため，処理手続の冗長性を緩和できる。

【０２０２】

（電子マネー入金システム）

図２４～図３１を参照しながら，本実施の形態にかかる決算システムにおける電子マネー入金システムおよびシーケンスについて説明することにする。

【０２０３】

本実施の形態にかかる決算システムにおいては，プリペイド方式の電子マネーとしてＩＣカード２０を利用するのであるが，ユーザ２はＩＣカード２０に記憶された価値情報の残高が不足した場合には，その残高を増やすように，価値情報の更新を行う必要がある。あるいは，場合によっては，ＩＣカード２０に記憶された価値情報を減額するように，価値情報の更新を行う必要がある。

【０２０４】

電子マネーをＩＣカードに入金する際には，ユーザ２は，リーダライタ２１によりＩＣカード２０にアクセス可能なパーソナルコンピュータ２０を介して決済管理装置３のアプリケーションサーバ（サイバー電子マネーシステム）３０にアクセスし，入金画面をディスプレイ上に表示するように要求する（①）。

【０２０５】

かかる入金画面要求を受けて，アプリケーションサーバ３０は，ＡｃｔｉｖｅＸコンポーネントなどの所定のインタフェースプログラム２４を介して，ユーザ２のパーソナルコンピュータ２０のディスプレイに，図２５に示すような入金画面が表示される（②）。

【０２０６】

ユーザ２が図２５に示す入金画面において，入金を選択すると，図２６に示すように，ＩＣカード２０をリーダライタ２１にセットするように指示がだされる。

【０２０７】

ユーザ２が，ＩＣカード２０をリーダライタ２１にセットすると，ＩＣカード２０内に記憶されている残高などが読み出され，サイバー電子マネーシステム３０に転送される（③）。また，同時に，カード内の履歴情報などもサイバー電子マネーシステムに吸い上げられる（④）。これらの処理が行われている間は，図２７に示すように，処理中である旨の表示がディスプレイに表示される。

【０２０８】

次いで，ユーザ２が，図２８および図２９に示されるような画面を参照しながら，パーソナルコンピュータ２２のキーボードやマウスなどを操作しながら，入

金金額，クレジットカードの番号や有効期限や暗証番号を入力してサイバー電子マネーシステムに転送する（③）。また，同時に，カード内の履歴情報などもサイバー電子マネーシステムに吸い上げられる（④）。これらの処理が行われている間は，図３０に示すように，処理中である旨の表示がディスプレイに表示される。

【０２０９】

サイバー電子マネーシステム３０は，上記のような入金要求情報を受けると，与信装置３５に対して，クレジット決済要求の承認を求める（⑤）。与信装置３５は，クレジット情報を精査した後，クレジット決済要求の可否を決定する。なお与信装置３５の詳細な構成については，本発明とは直接的な関係を有しないので，詳細な説明は省略することにする。

【０２１０】

与信の結果が肯定的である場合には，サイバー電子マネーシステムは，価値更新情報を生成する。サイバー電子マネーシステムは，価値更新情報を，決済管理装置３とＩＣカード２０との間で共用される共通鍵により暗号化する。

【０２１１】

さらに，価値更新情報は，決済管理装置３の秘密鍵により作成される第５署名を付されて，ユーザ２のパーソナルコンピュータ２２に送信される。ユーザ２のパーソナルコンピュータ２２は，決済管理装置３の秘密鍵に対応する公開鍵により，送られてきた価値更新情報の正当性を検証し，正しいものであれば，その価値更新情報を決済管理装置３とＩＣカード２０との間で共用される共通鍵により復号化する。そして，復号化された価値更新情報に基づいてＩＣカード２０内の価値情報を更新する（⑥）。

【０２１２】

パーソナルコンピュータ２２は，サイバー電子マネーシステム３０に対して入金完了画面要求を送信し（⑦），図３１に示すような，入金完了画面がパーソナルコンピュータ２２のディスプレイに表示される（⑧）。その後，図３２に示すように，サイバー電子マネーシステムのトップページに復帰して，一連の価値更新処理が完了する。

【０２１３】

なお，一連の処理に関するカードログ情報は，バッチ処理で，精査・決済システム用の情報管理サーバ３２に送られて，保存される。

【０２１４】

以上説明したように，本実施の形態にかかる決済システムを利用した電子マネー入金システムによれば，ＩＣカード２０のメモリ５２に共通鍵KCを記憶し，秘密鍵は記憶しない。そのため，ユーザ２がＩＣカード２０を紛失した場合でも，メモリ５２には秘密鍵が記憶されていないため，秘密鍵を用いてユーザ２の署名が不正に行われることを回避できる。

【０２１５】

また，電子決済システム１によれば，共通鍵はＩＣカード２０およびセキュリティサーバ３１の内部でのみ使用されることから，共通鍵が盗まれる危険性を低くでき，安全な入金処理を実現できると共に，鍵管理を容易にすることができる。

【０２１６】

以上，添付図面を参照しながら本発明にかかる電子決済システム等の好適な実施形態について説明したが，本発明はかかる例に限定されない。当業者であれば，特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり，それらについても当然に本発明の技術的範囲に属するものと了解される。

【０２１７】

例えば，上述した実施形態では，図１に示すように，決済管理装置３において，アプリケーションサーバ３０，セキュリティサーバ３１および情報管理サーバ３２を別々に設けた場合を例示したが，これらのサーバの機能を一つのサーバで実現してもよい。

【０２１８】

また，上述した実施形態では，ＩＣカード２０内の残高情報をアプリケーションサーバ３０に読み出す場合を例示したが，当該残高情報をアプリケーションサーバ３０に読み出さないようにしてもよい。

【０２１９】

【発明の効果】　以上説明したように，本発明によれば，共通鍵を保持したＩＣカードを用いて，ネットワークを介した電子商取引を安全に行う電子決済システム，決済管理装置，店舗装置，クライアント装置，ＩＣカード，コンピュータプログラムおよび記憶媒体を提供できる。

【０２２０】

特に，本発明にかかる電子決済システム等によれば，ＩＣカード２０のメモリ５２に共通鍵を記憶し，秘密鍵は記憶しない。そのため，ユーザがＩＣカードを紛失した場合でも，メモリには秘密鍵が記憶されていないため，秘密鍵を用いてユーザの署名が不正に行われることを回避できる。

【０２２１】

また，本発明にかかる電子決済システム等によれば，共通鍵はＩＣカードおよびセキュリティサーバの内部でのみ使用されることから，共通鍵が盗まれる危険性を低くでき，安全な取り引きを実現できると共に，鍵管理を容易にすることができる。

【０２２２】

また，本発明にかかる電子決済システム等によれば，ネットワークを流通する各種情報および要求を送受信する際に，秘密鍵および公開鍵を用いた署名検証を行うことから，当該情報および要求がネットワーク上で不正に改竄されることを回避でき，ネットワークを用いた取り引きの安全性を確保できる。

【０２２３】

このように，本発明にかかる電子決済システム等によれば，決済処理や入金処理に伴う手順を従来に比べて少なくでき，ネットワークを介した情報伝送を削減でき，ネットワークの利用量の削減，並びに処理時間を短縮を図れる。

【図面の簡単な説明】

【図１】　図１は，本発明の一実施形態にかかる電子決済システムの全体構成図である。

【図２】　図２は，図１に示すＩＣカードの構成を説明するための概略的な説明図である。

【図３】　図３は，本発明の実施形態にかかる電子決済システムの別の構成例を示す構成図である。

【図４】　図４は，本発明の実施形態にかかる電子決済システムにおける情報の流れを示す構成図である。

【図５】　ユーザのＩＣカードと，決済管理装置のセキュリティサーバとの間の通信方法を説明するための図である。

【図６】　ユーザのパーソナルコンピュータと，店舗のネットワークサーバとの間の通信方法を説明するための図である。

【図７】　ユーザのパーソナルコンピュータと，決済管理装置のアプリケーションサーバとの間の通信方法を説明するための図である。

【図８】　本発明の実施形態にかかる電子決済システムの電子マネー出金の流れを示す説明図である。

【図９】　図１に示す電子決済システムの動作を説明するための図であり，商品情報伝送シーケンスを示している。

【図１０】　図１に示す電子決済システムの動作を説明するための図であり，価値情報伝送シーケンスを示している。

【図１１】　図１に示す電子決済システムの動作を説明するための図であり，価値情報伝送シーケンスを示している。

【図１２】　図１に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図１３】　図１に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図１４】　図１に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図１５】　図１に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図１６】　図１に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図１７】　図１に示す電子決済システムの決済動作中にクライアント装置

に表示される画面構成例である。

【図１８】　図１に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図１９】　図１に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図２０】　図１に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図２１】　図１に示す電子決済システムの動作を説明するための図であり，商品情報伝送シーケンスを示している。

【図２２】　図１に示す電子決済システムの動作を説明するための図であり，価値情報伝送シーケンスを示している。

【図２３】　図１に示す電子決済システムの動作を説明するための図であり，価値情報伝送シーケンスを示している。

【図２４】　本発明の実施形態にかかる電子決済システムの電子マネー入金の流れを示す説明図である。

【図２５】　図１に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図２６】　図１に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図２７】　図１に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図２８】　図１に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図２９】　図１に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図３０】　図１に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図３１】　図１に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図３２】　図１に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【符号の説明】　１…電子決済システム，

２…ユーザ，

３…決済管理装置，

４…店舗装置，

５…ネットワーク，

２０…ＩＣカード，

２１…ＩＣカードリーダライタ，

２２…パーソナルコンピュータ，

２３…ブラウザプログラム，

２４…インタフェースプログラム，

３０…アプリケーションサーバ，

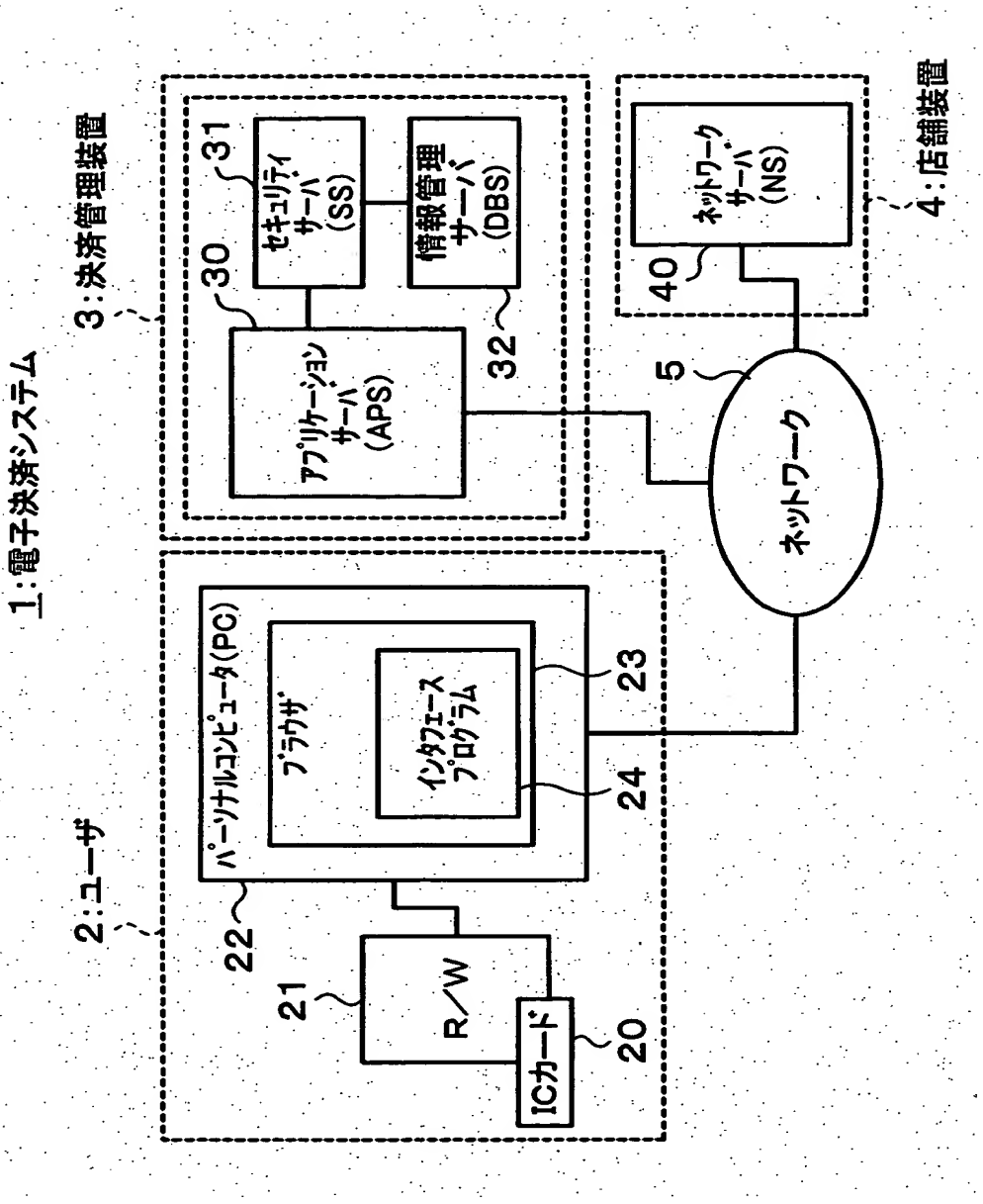
３１…セキュリティサーバ，

３２…情報管理サーバ，

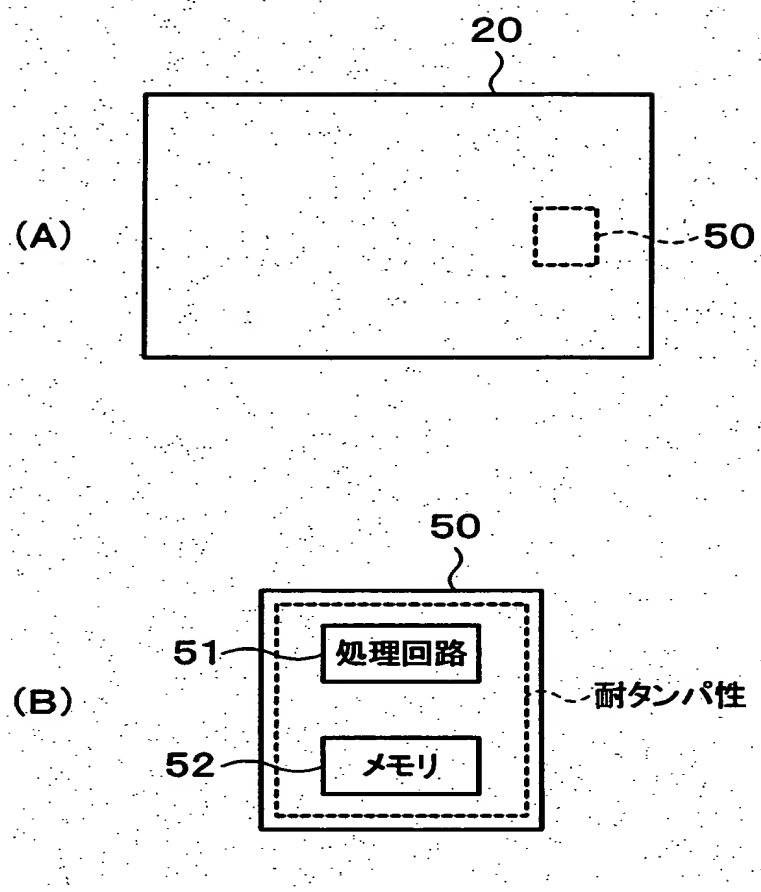
４０…ネットワークサーバ

【書類名】　　図面

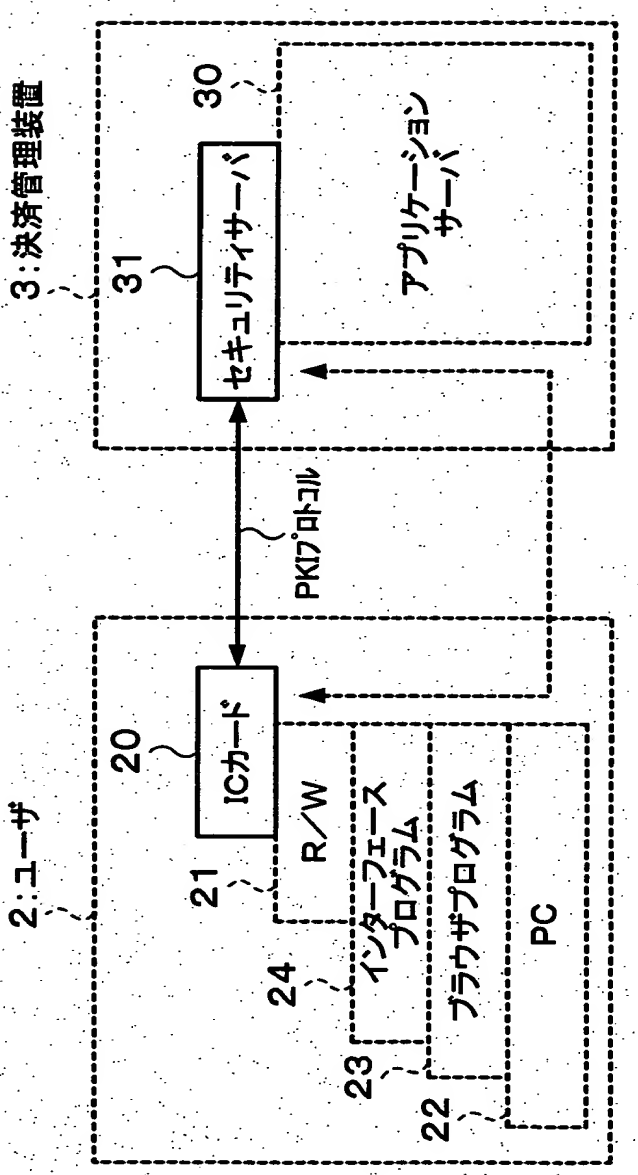
【図１】


1:電子決済システム
3:決済管理装置
31
セキュリティサーバ(SS)
情報管理サーバ(DBS)
30
32
アプリケーションサーバ(APS)
4:店舗装置
ネットワークサーバ(NS)
40
5
ネットワーク
2:ユーザ
パーソナルコンピュータ(PC)
ブラウザ
インタフェースプログラム
23
24
22
21
R/W
ICカード
20

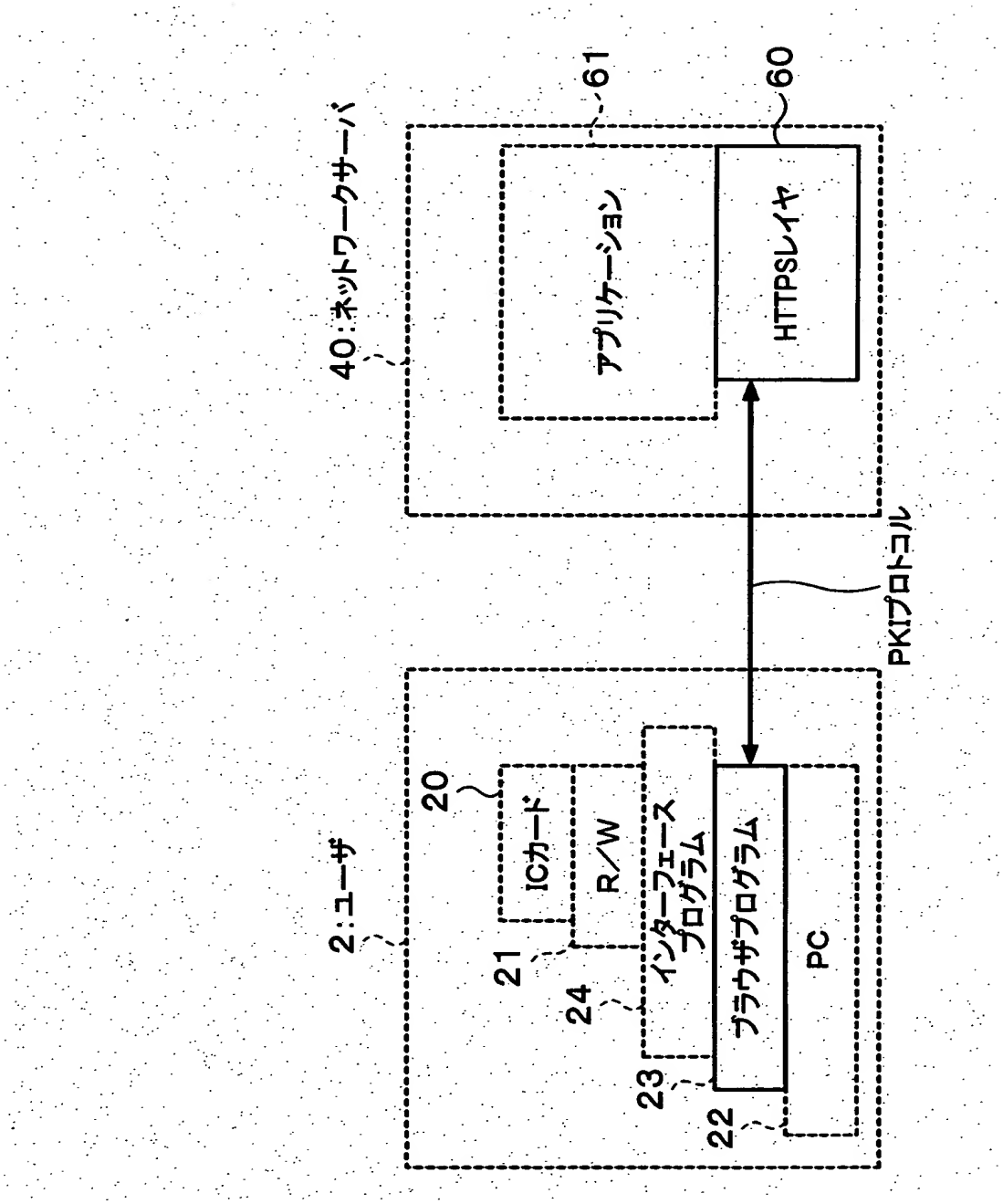
【図２】



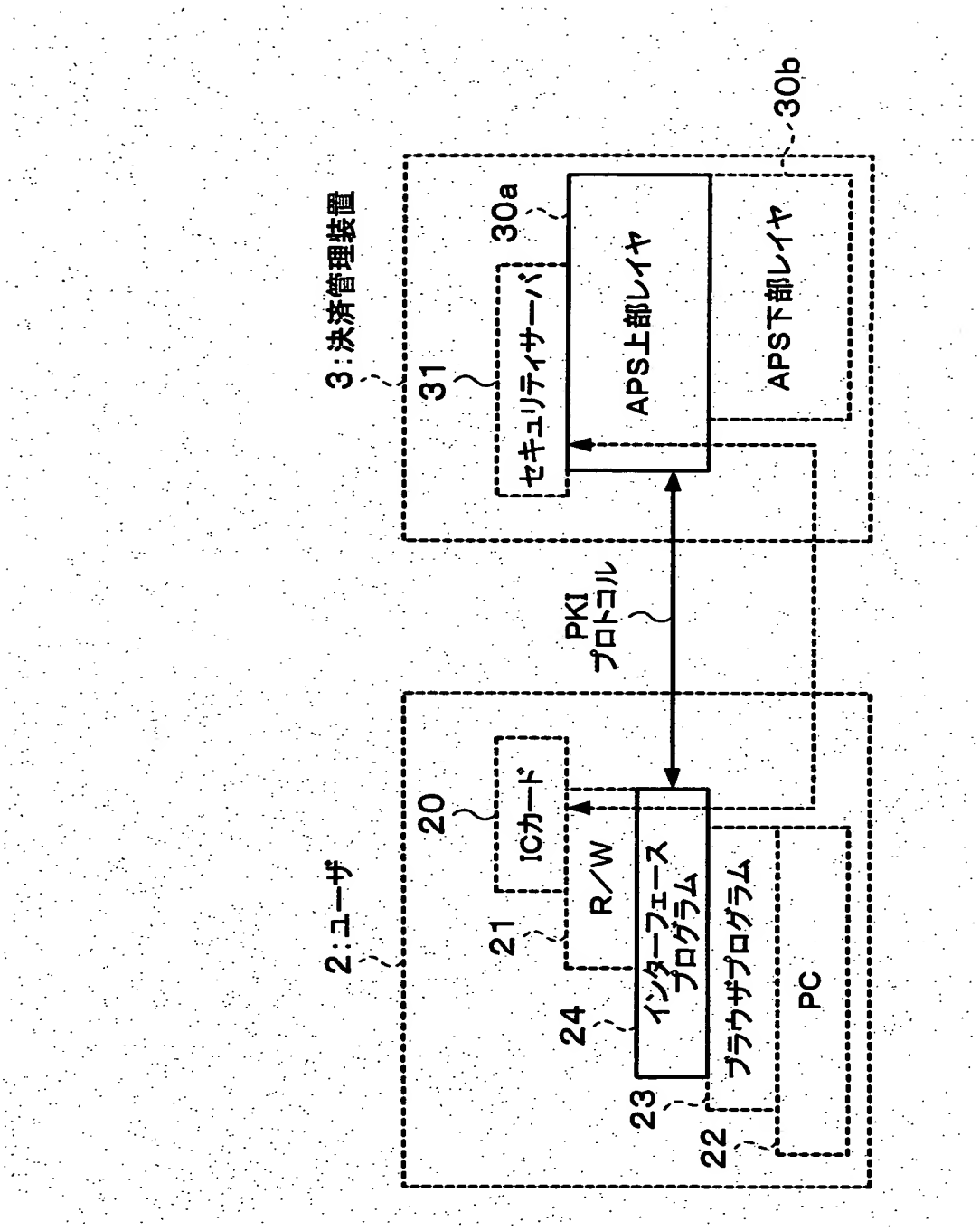
【図３】


3:決済管理装置
30
アプリケーション
サーバ
31
セキュリティサーバ
PKIプロトコル
2:ユーザ
20
ICカード
21
R/W
24
インターフェース
プログラム
23
ブラウザプログラム
22
PC

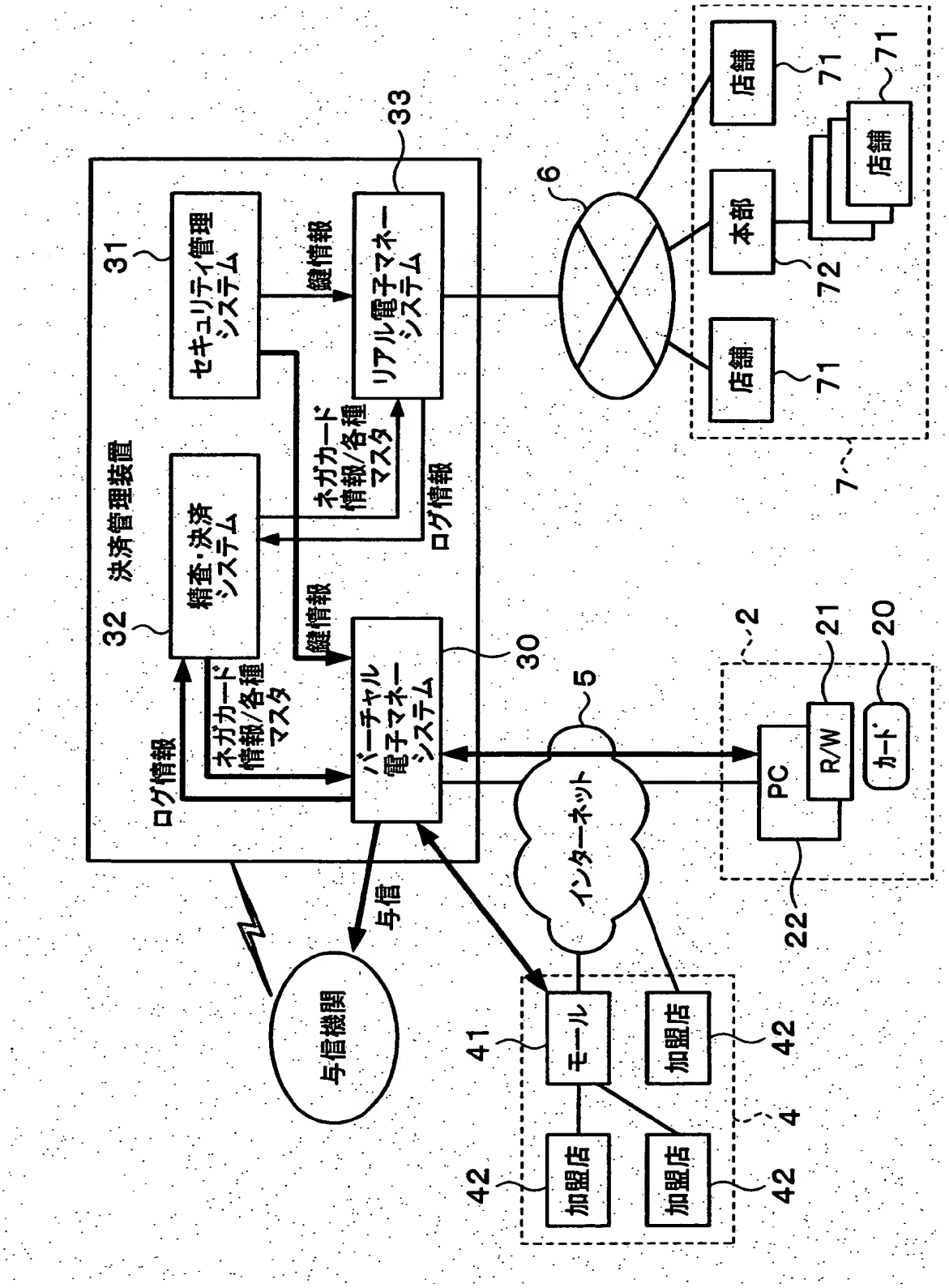
【図４】


40:ネットワークサーバ
61
60
アプリケーション
HTTPSレイヤ
PKIプロトコル
2:ユーザ
20
ICカード
R/W
インターフェース
プログラム
ブラウザプログラム
PC
21
24
23
22

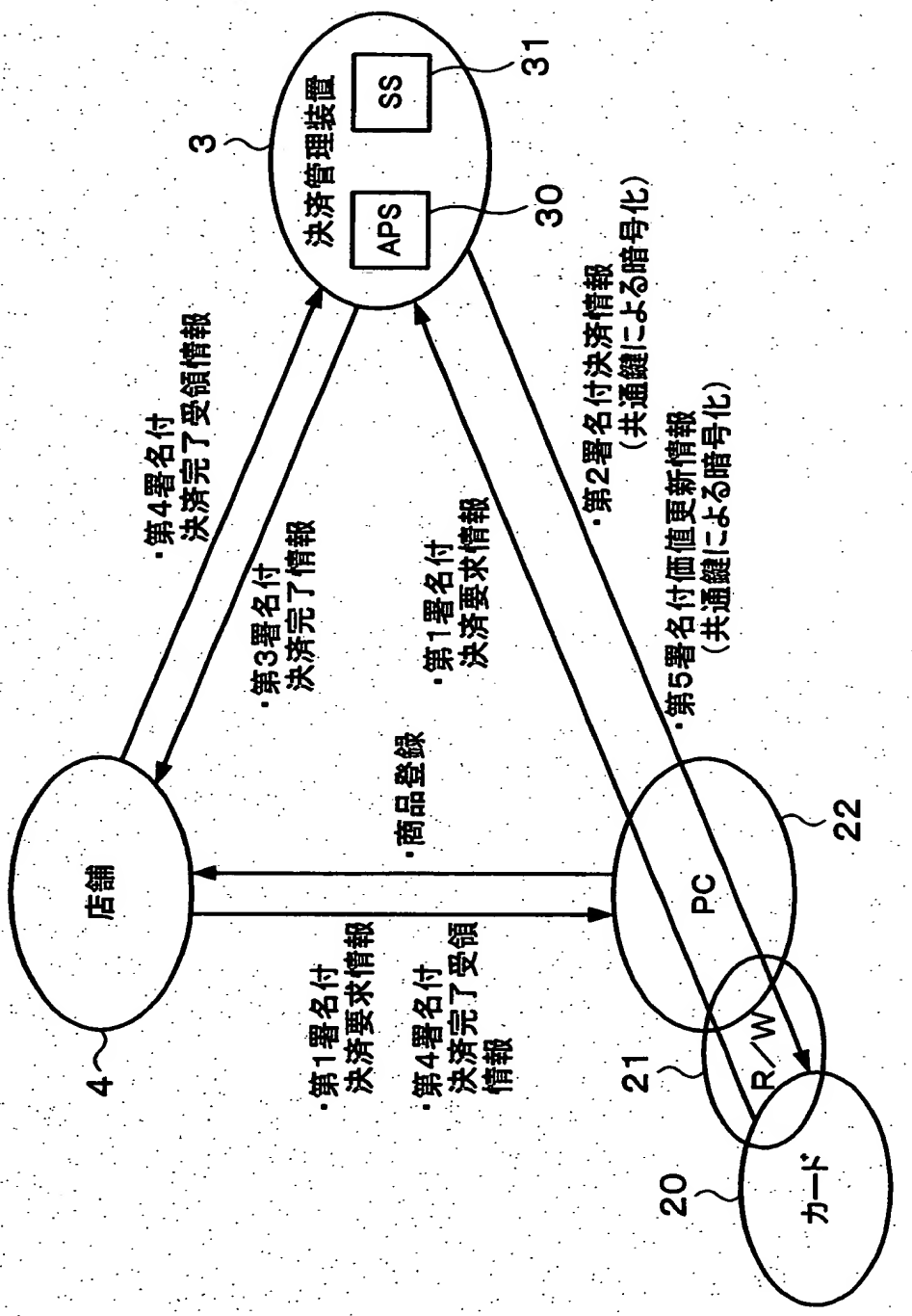
【図５】


3:決済管理装置
30b
30a
31
セキュリティサーバ
APS上部レイヤ
APS下部レイヤ
PKI
プロトコル
2:ユーザ
20
ICカード
21
R／W
24
インターフェース
プログラム
23
ブラウザプログラム
22
PC

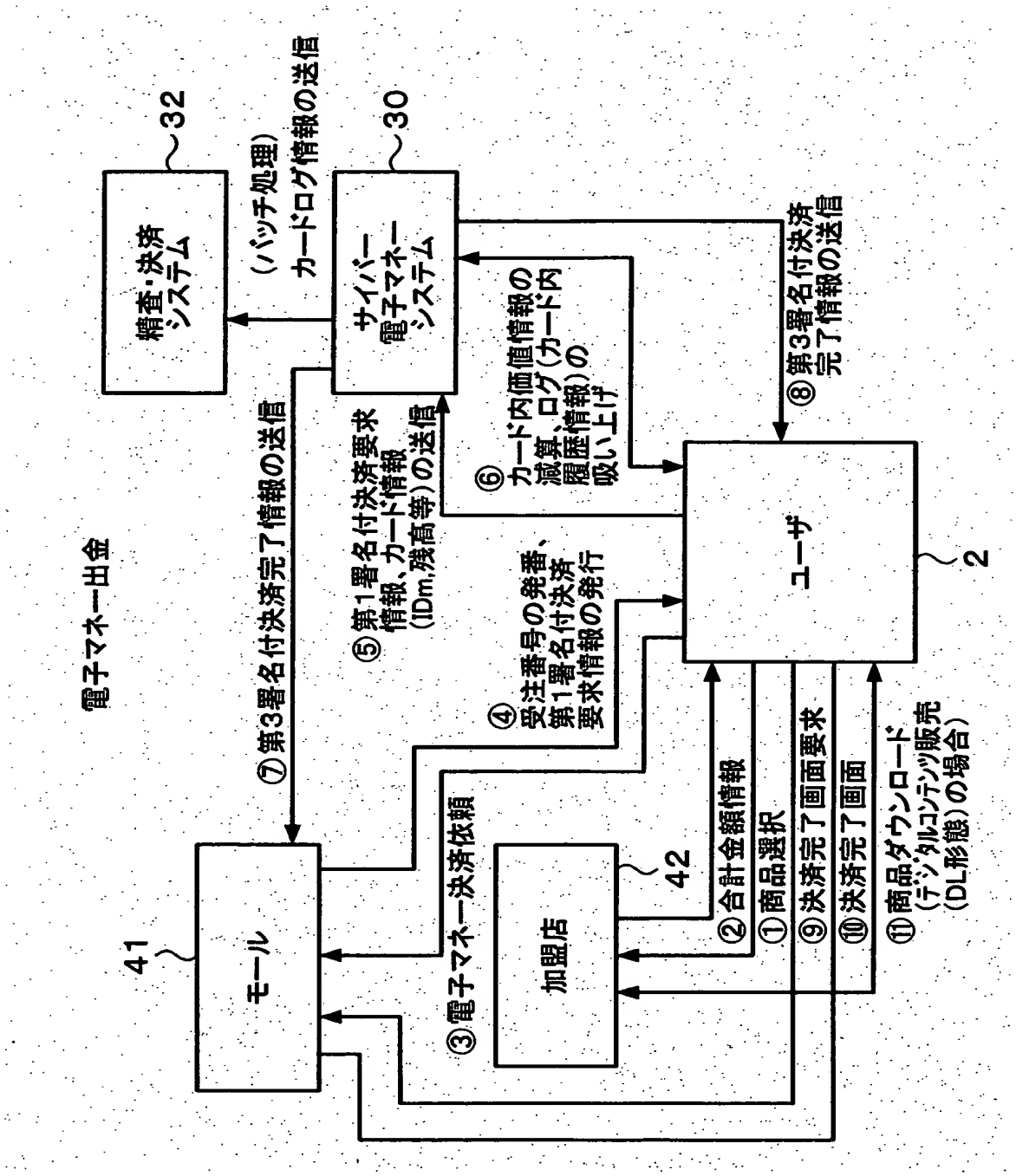
【図６】


決済管理装置
32
31
33
セキュリティ管理システム
鍵情報
リアル電子マネーシステム
精査・決済システム
ネガカード情報/各種マスタ
ログ情報
鍵情報
ネガカード情報/各種マスタ
ログ情報
バーチャル電子マネーシステム
30
6
店舗
71
店舗
71
本部
72
店舗
71
7
2
21
20
PC
R/W
カード
22
5
インターネット
与信
与信機関
41
モール
加盟店
42
加盟店
42
加盟店
42
4

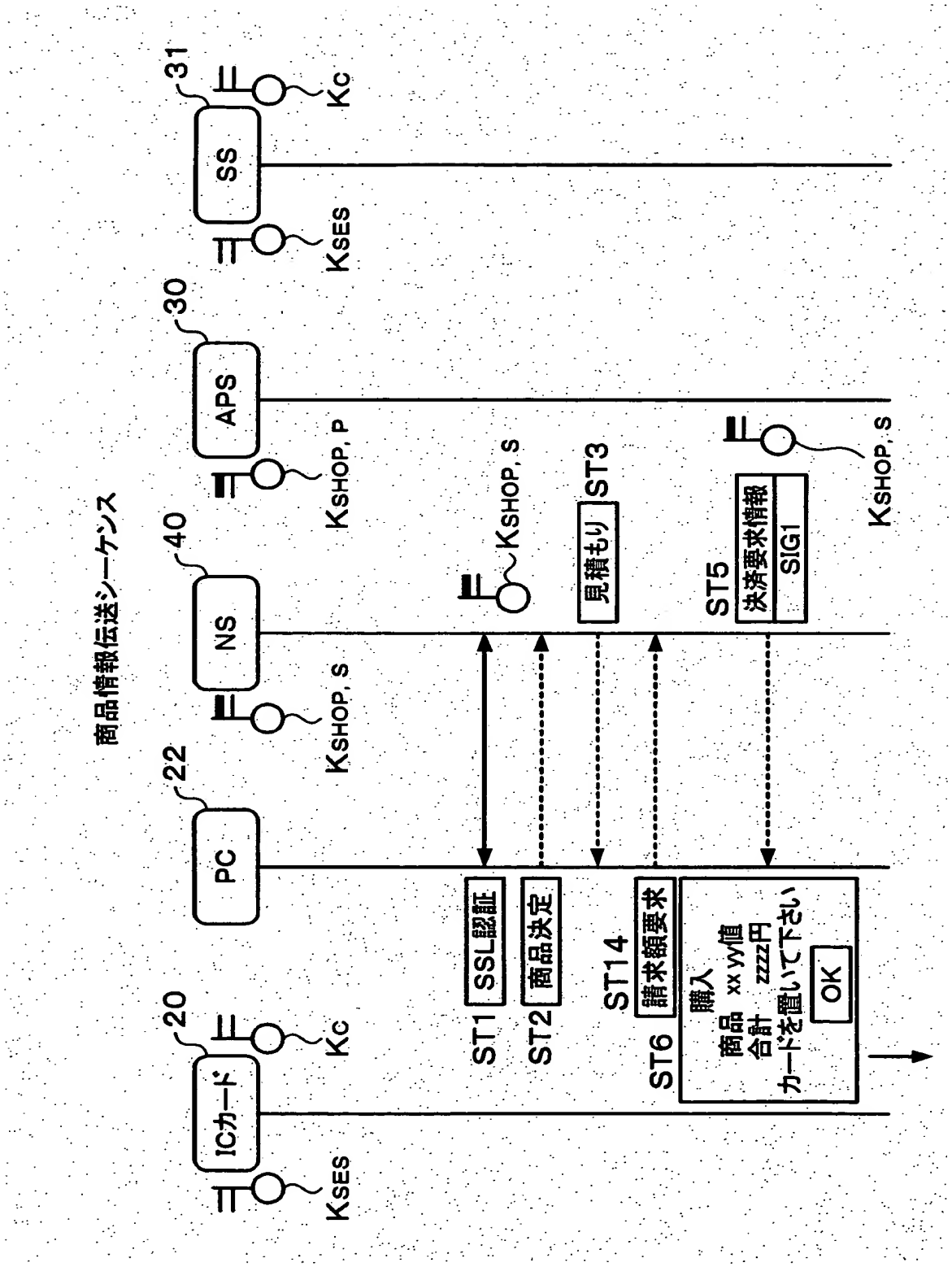
【図７】


決済管理装置
SS
APS
3
31
30
店舗
4
PC
22
R／W
21
カード
20
・第4署名付
決済完了受領情報
・第3署名付
決済完了情報
・第1署名付
決済要求情報
・第2署名付決済情報
（共通鍵による暗号化）
・第5署名付価値更新情報
（共通鍵による暗号化）
・商品登録
・第1署名付
決済要求情報
・第4署名付
決済完了受領
情報

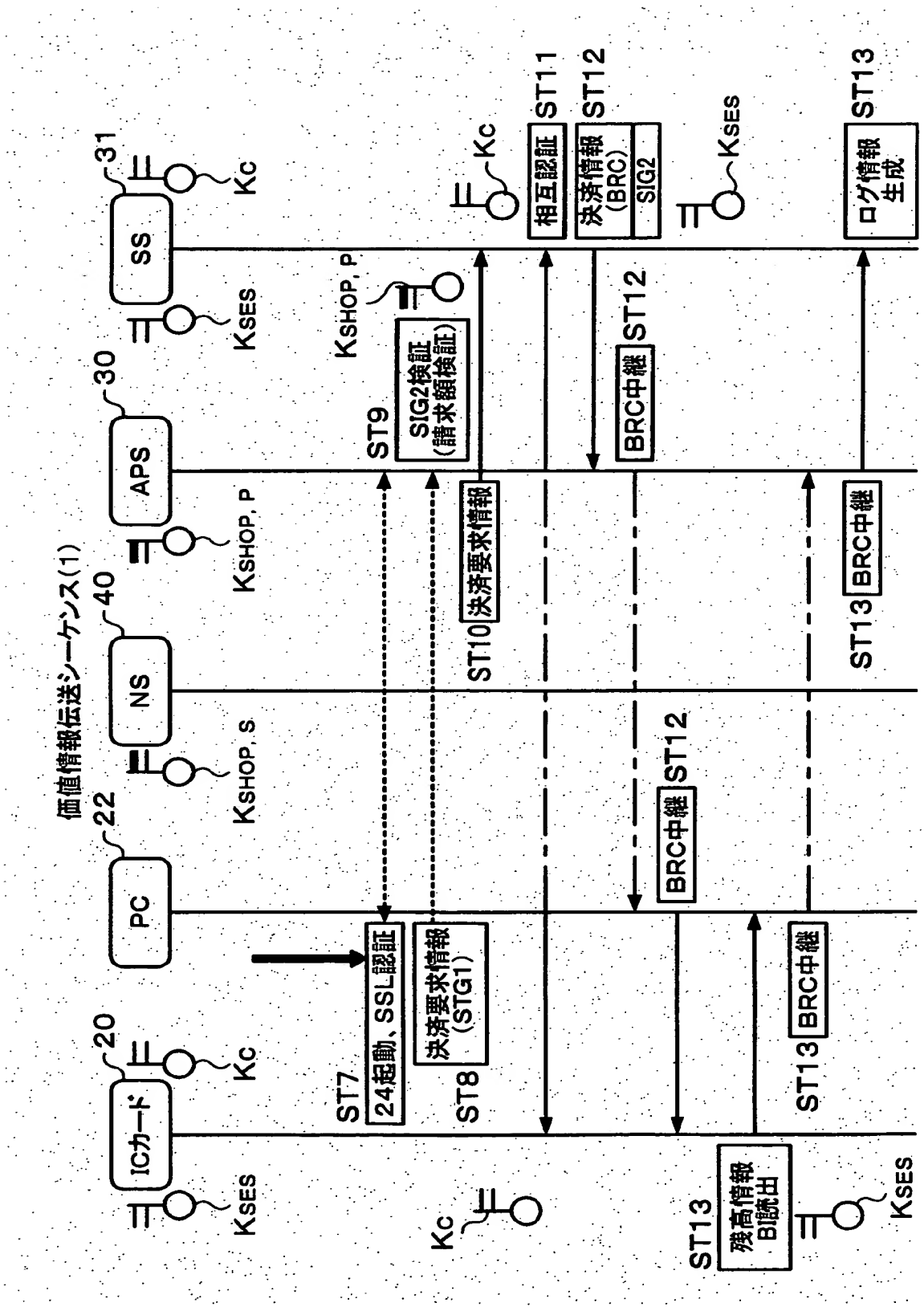
【図８】


精査・決済システム
32
（バッチ処理）
カードログ情報の送信
サイバー電子マネーシステム
30
⑧第3署名付決済完了情報の送信
⑥カード内価値情報の減算、ログ（カード内履歴情報）の吸い上げ
⑤第1署名付決済要求情報、カード情報（IDm,残高等）の送信
⑦第3署名付決済完了情報の送信
電子マネー出金
④受注番号の発番、第1署名付決済要求情報の発行
ユーザ
2
③電子マネー決済依頼
②合計金額情報
①商品選択
⑨決済完了画面要求
⑩決済完了画面
⑪商品ダウンロード（デジタルコンテンツ販売（DL形態）の場合）
モール
41
加盟店
42

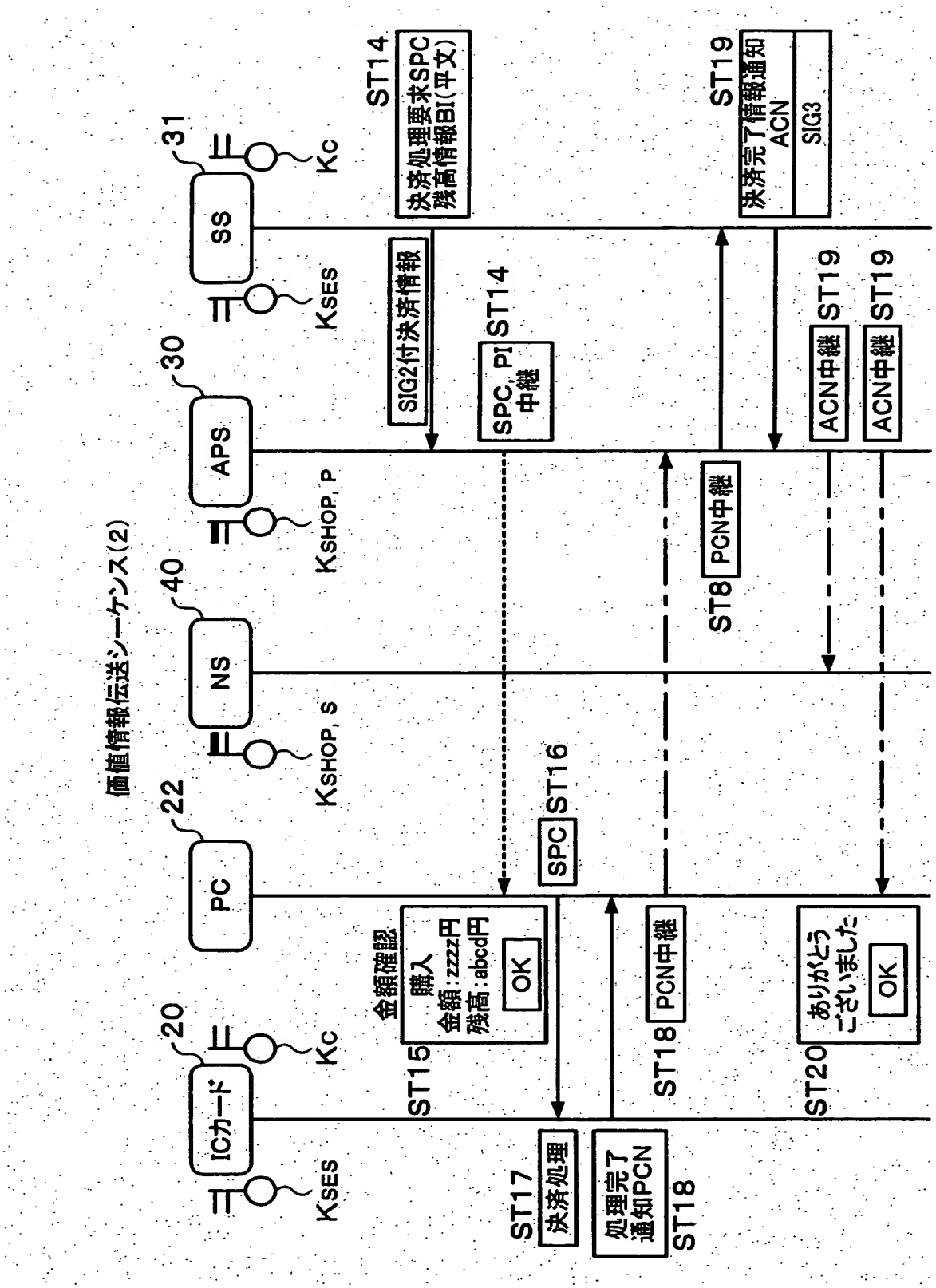
【図９】


商品情報伝送シーケンス
20
ICカード
Kc
KSES
22
PC
40
NS
KSHOP, S
30
APS
KSHOP, P
31
SS
KSES
KSHOP, S
ST1
SSL認証
ST2
商品決定
ST3
見積もり
ST5
決済要求情報
SIG1
ST14
請求額要求
ST6
購入
商品 xx yy値
合計 zzzz円
カードを置いて下さい
OK

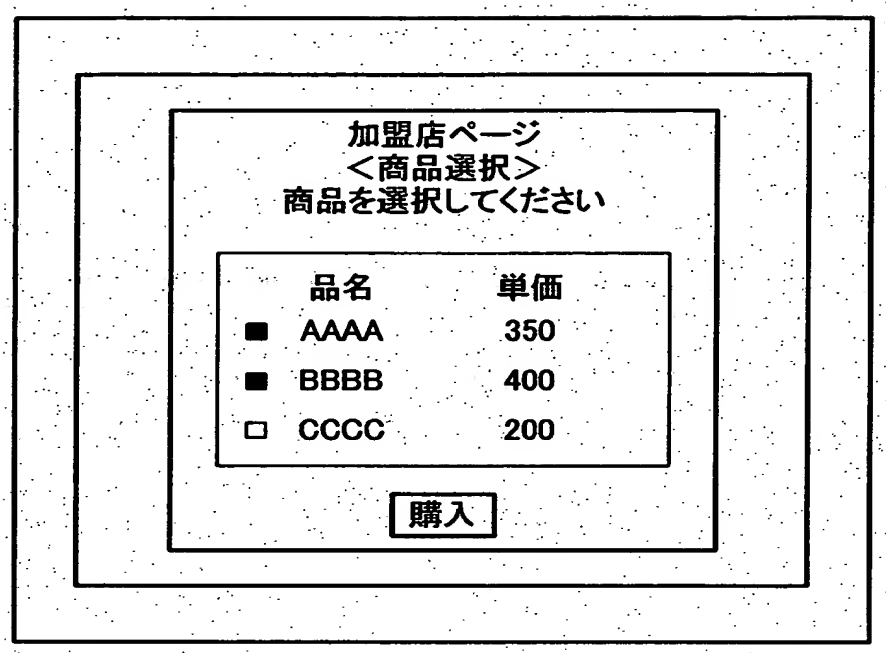
【図１０】


価値情報伝送シーケンス(1)
ICカード
20
PC
22
NS
40
APS
30
SS
31
KSES
KC
KSHOP, S
KSHOP, P
ST7
24起動、SSL認証
ST8
決済要求情報
(STG1)
ST9
SIG2検証
(請求額検証)
ST10
決済要求情報
ST11
相互認証
ST12
決済情報
(BRC)
SIG2
BRC中継
ST13
残高情報
BI読出
ログ情報
生成

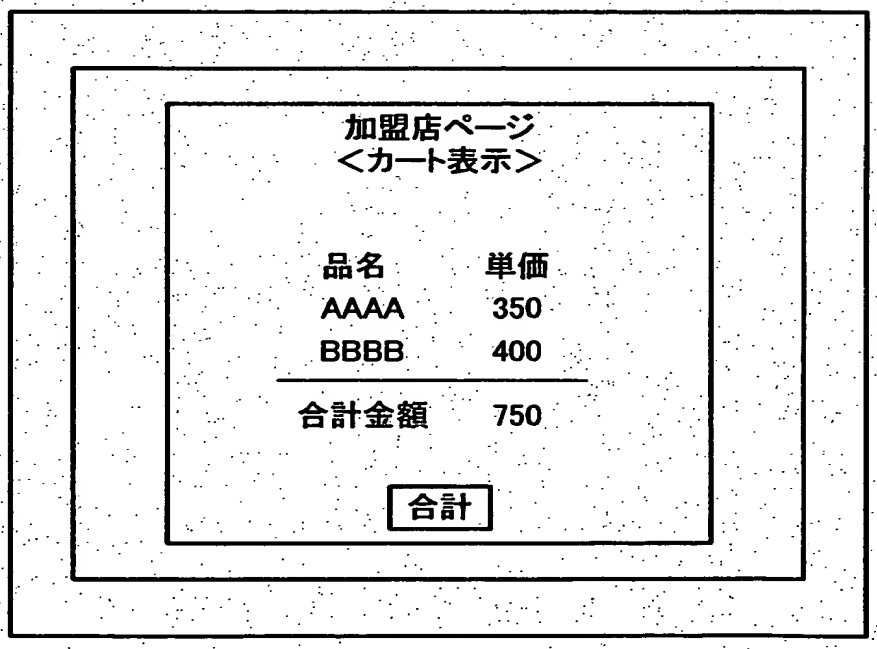
【図１１】


価値情報伝送シーケンス(2)
20
ICカード
Kc
KSES
22
PC
KSHOP, S
40
NS
KSHOP, P
30
APS
KSES
31
SS
Kc
ST14
決済処理要求SPC
残高情報BI(平文)
SIG2付決済情報
SPC, PI
中継
ST14
ST19
決済完了情報通知
ACN
SIG3
ACN中継
ST19
ACN中継
ST19
PCN中継
ST8
SPC
ST16
金額確認
購入
金額：zzzz円
残高：abcd円
OK
ST15
PCN中継
ST18
ありがとう
ございました
OK
ST20
決済処理
ST17
処理完了
通知PCN
ST18

【図１２】

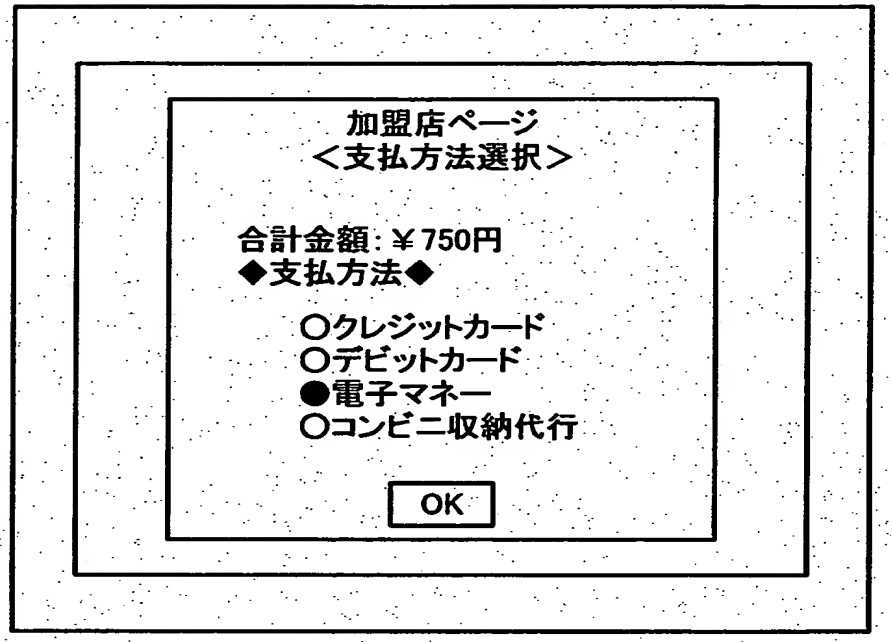


【図１３】

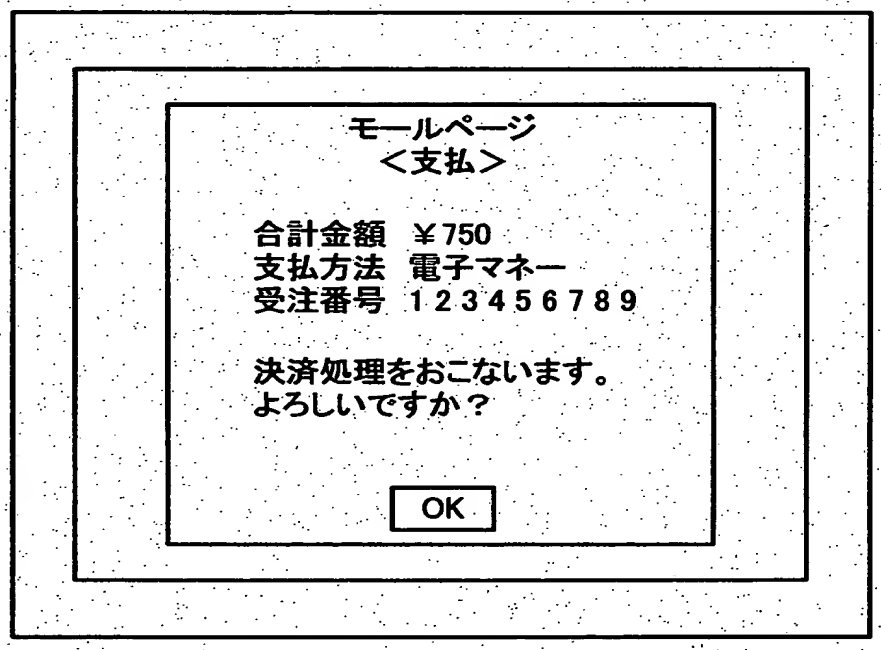


出証特２００１－３０４７３４７

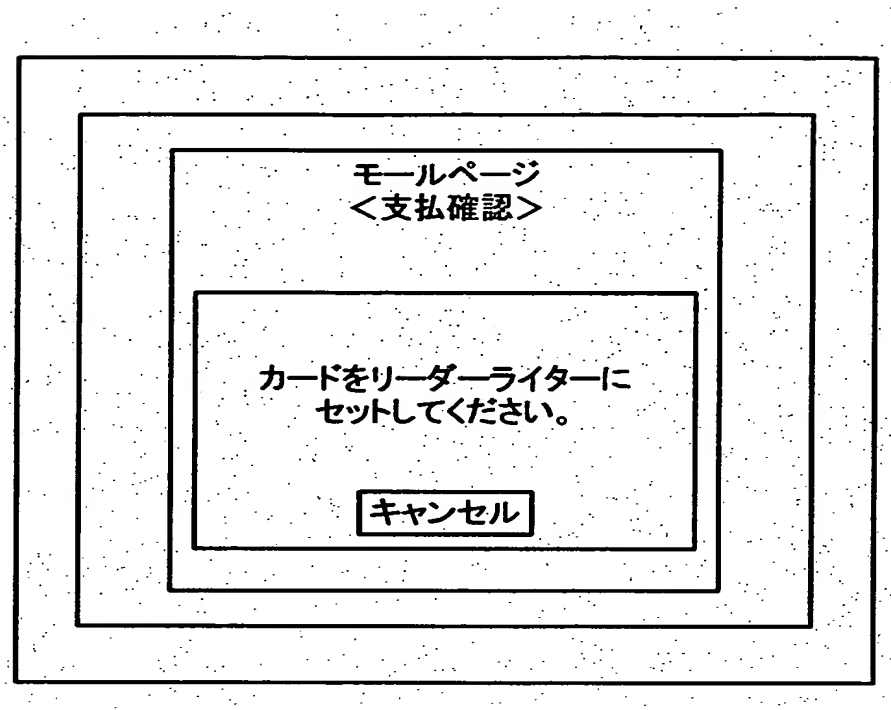
【図１４】


加盟店ページ
＜支払方法選択＞
合計金額：￥750円
◆支払方法◆
○クレジットカード
○デビットカード
●電子マネー
○コンビニ収納代行
OK

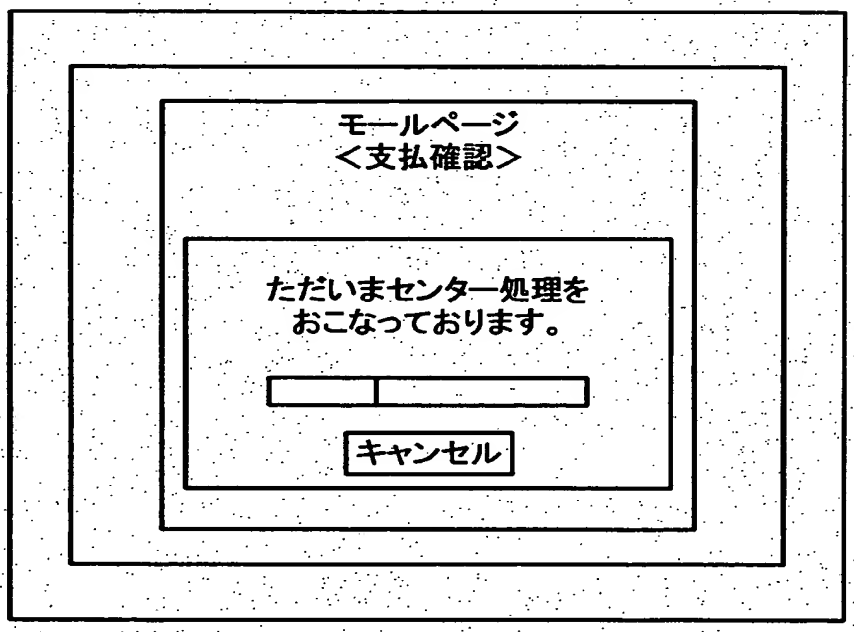
【図１５】


モールページ
＜支払＞
合計金額　￥750
支払方法　電子マネー
受注番号　１２３４５６７８９
決済処理をおこないます。
よろしいですか？
OK

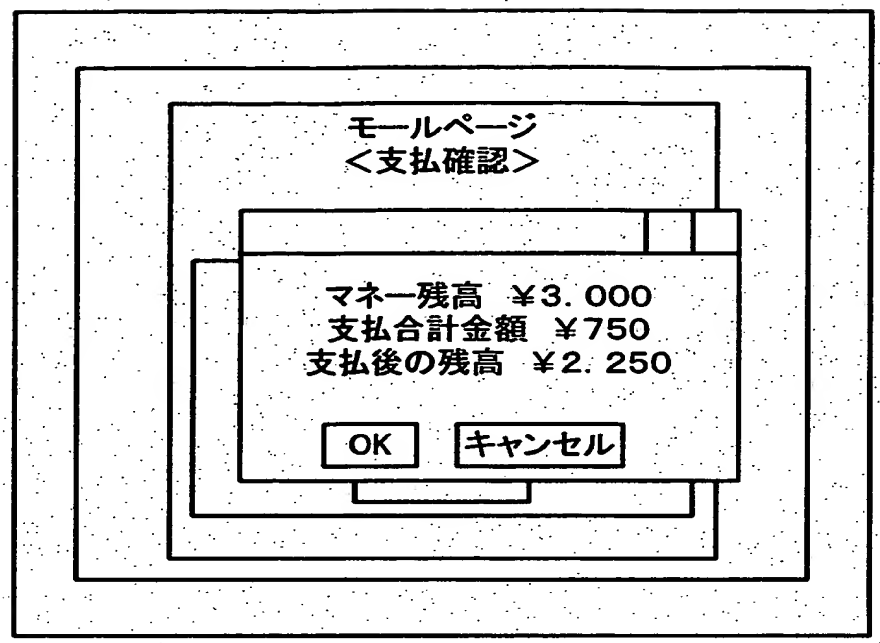
【図１６】


モールページ
＜支払確認＞
カードをリーダーライターに
セットしてください。
キャンセル

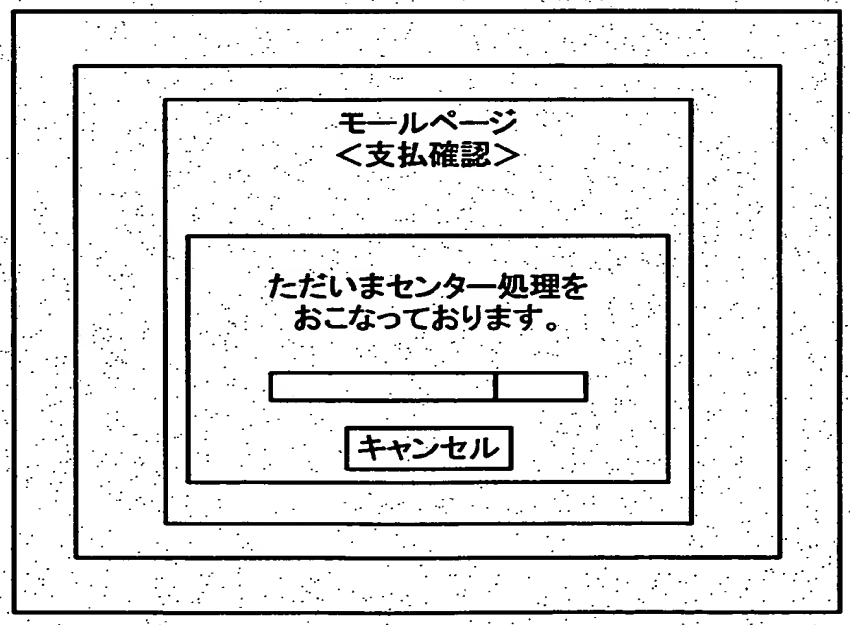
【図１７】


モールページ
＜支払確認＞
ただいまセンター処理を
おこなっております。
キャンセル

【図１８】

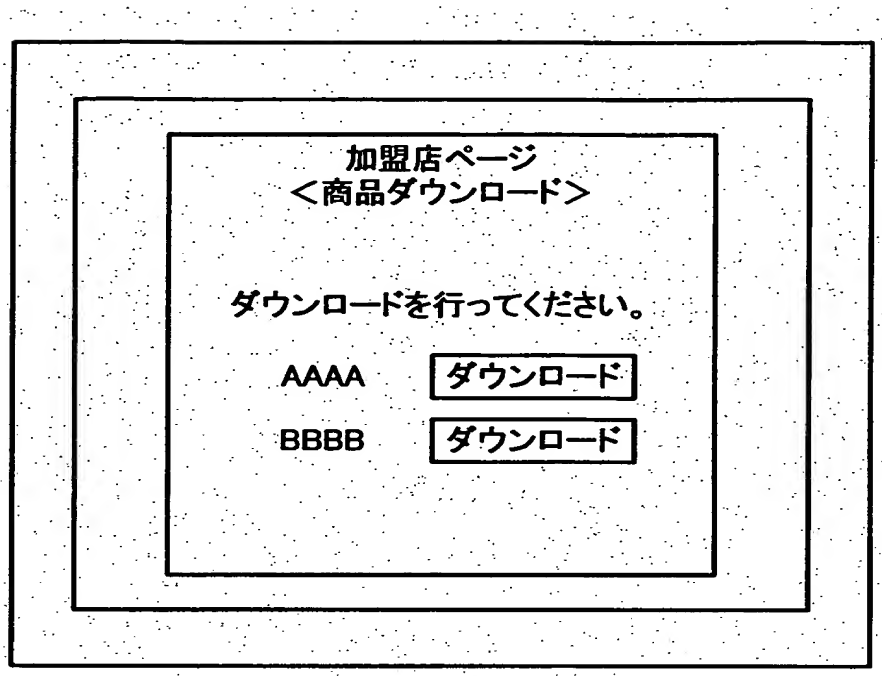


【図１９】

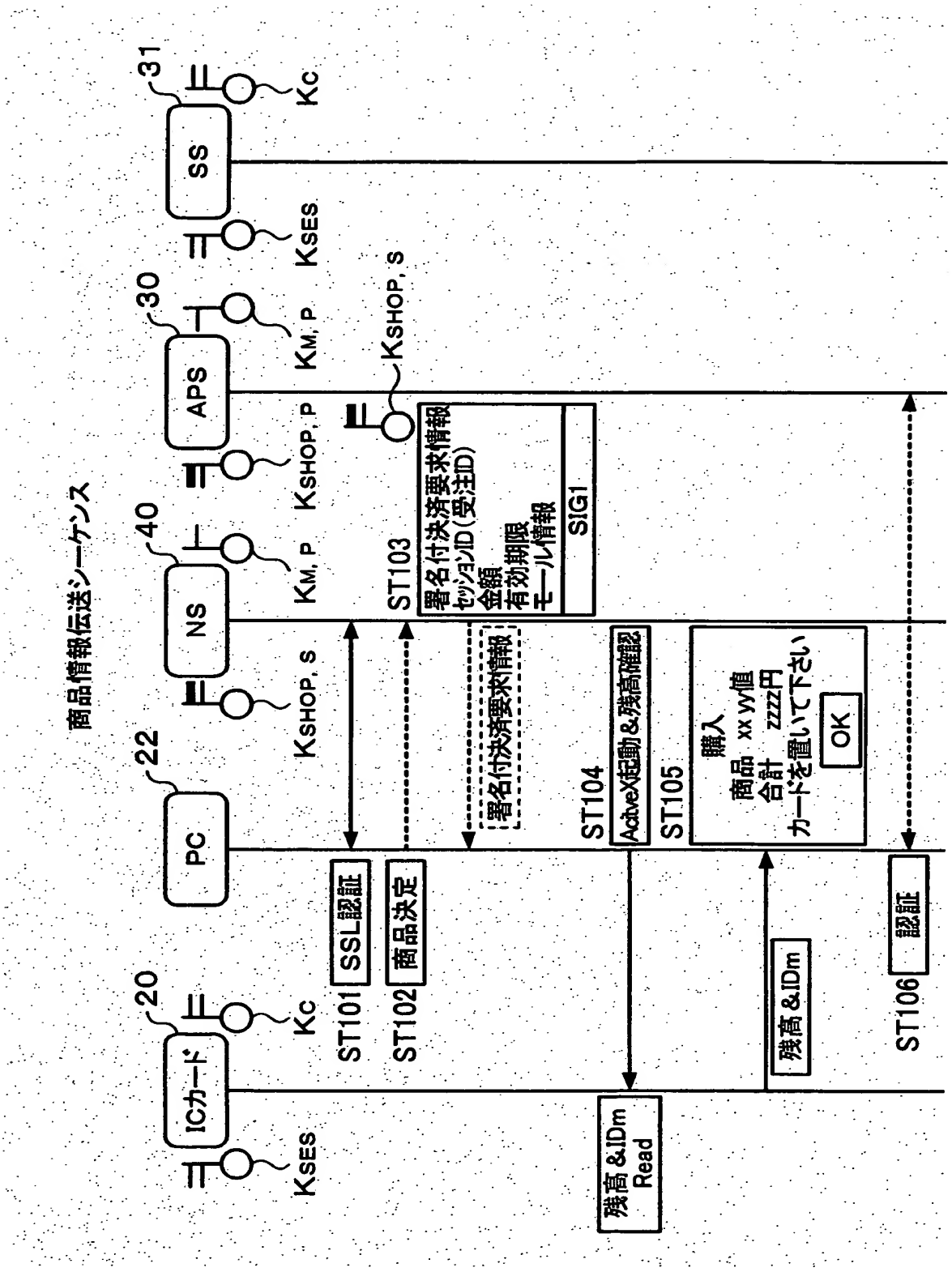


出証特２００１－３０４７３４７

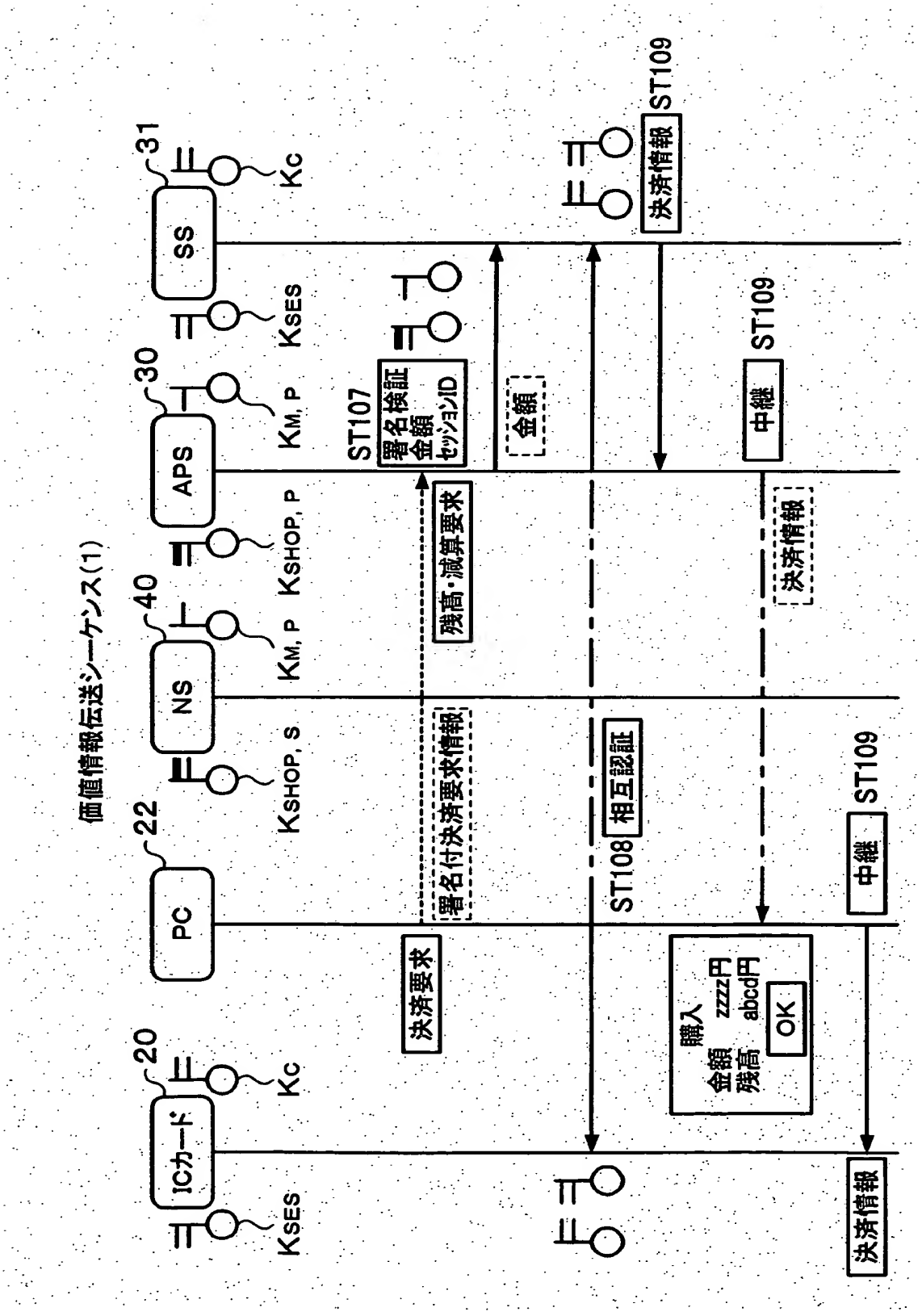
【図２０】



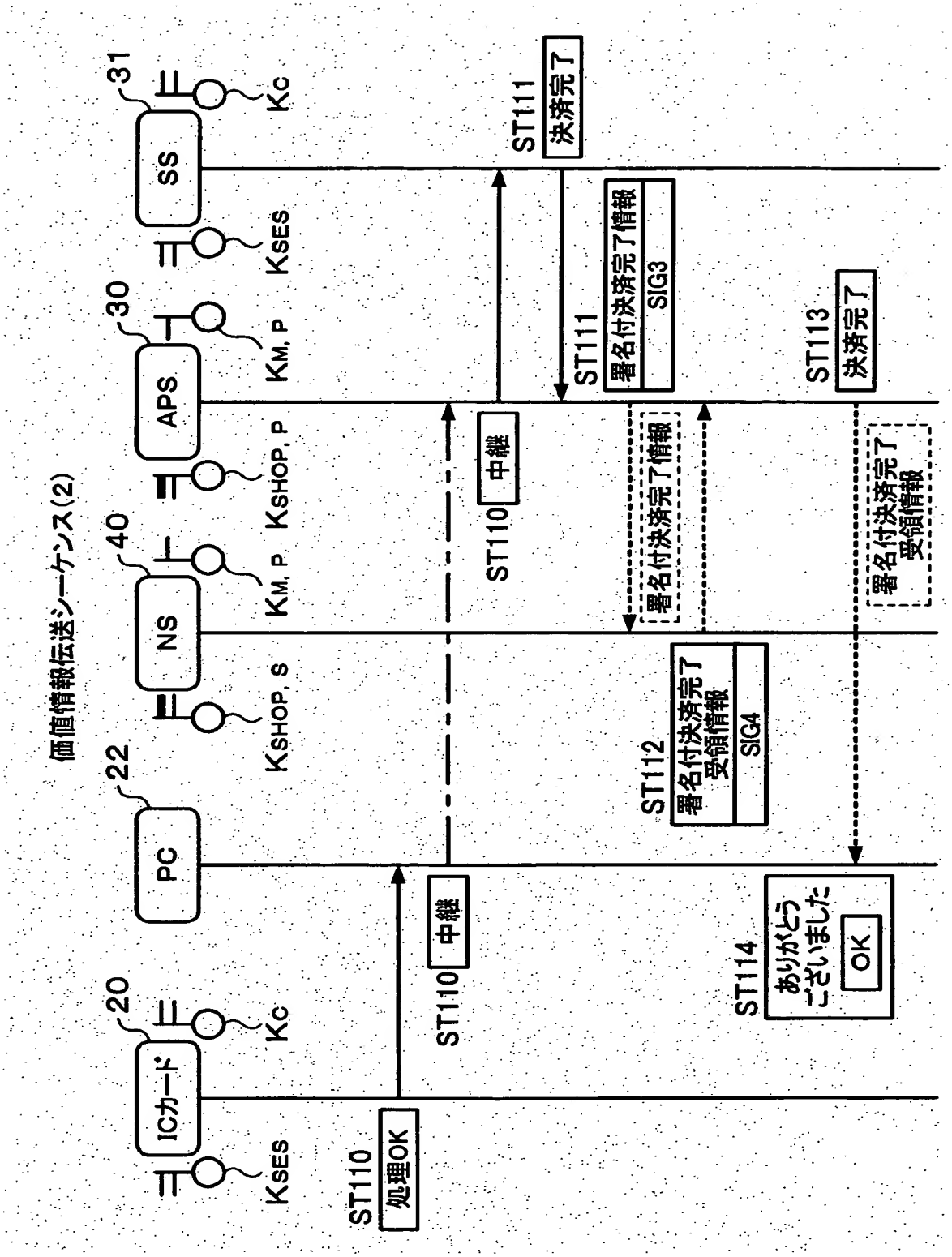
【図２１】


商品情報伝送シーケンス
ICカード
20
PC
22
NS
40
APS
30
SS
31
Kc
KSES
KM, P
KSHOP, P
KSHOP, S
ST101
SSL認証
ST102
商品決定
ST103
署名付決済要求情報
セッションID(受注ID)
金額
有効期限
モール情報
SIG1
署名付決済要求情報
ST104
Active起動&残高確認
ST105
購入
商品 xx yy値
合計 zzzz円
カードを置いて下さい
OK
残高 &IDm
Read
残高 &IDm
ST106
認証

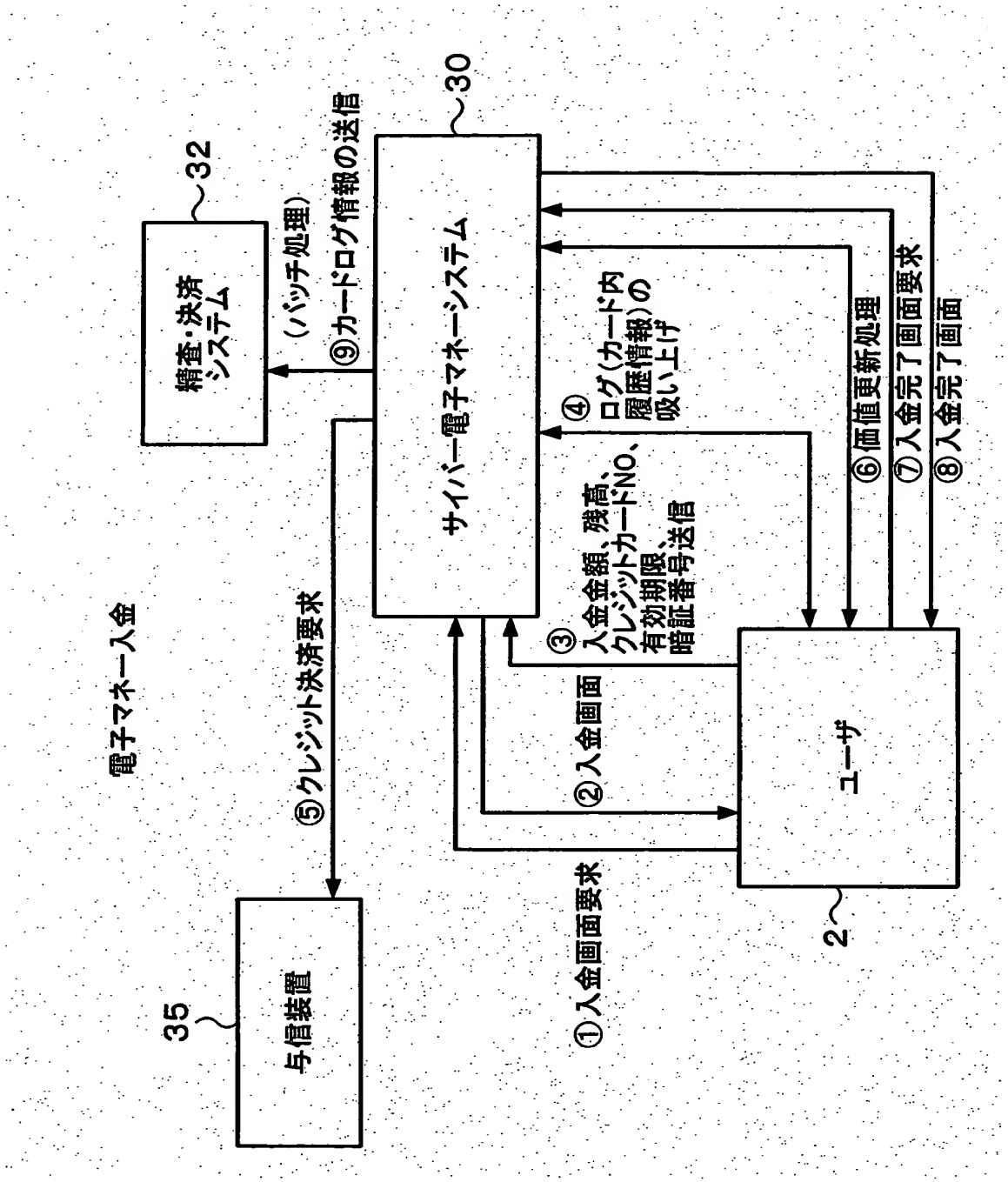
【図２２】


価値情報伝送シーケンス(1)
ICカード
20
PC
22
NS
40
APS
30
SS
31
Kc
KSES
KSHOP, S
KM, P
KSHOP, P
KM, P
Kc
KSES
決済要求
署名付決済要求情報
残高・減算要求
ST107
署名検証
金額
セッションID
金額
ST108
相互認証
購入
金額 zzzz円
残高 abcd円
OK
中継
ST109
決済情報
ST109
中継
ST109
決済情報

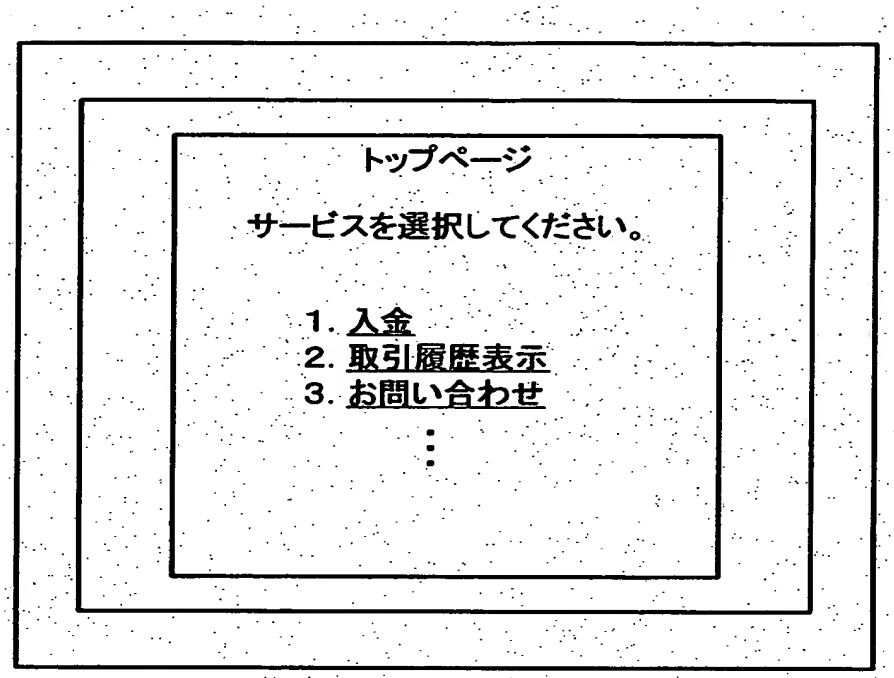
【図２３】


価値情報伝送シーケンス(2)
ICカード
20
PC
22
NS
40
APS
30
SS
31
KSES
Kc
KSHOP, S
KM, P
KSHOP, P
ST110
処理OK
中継
署名付決済完了情報
SIG4
ST111
決済完了
署名付決済完了情報
SIG3
ST112
ST113
決済完了
署名付決済完了
受領情報
ST114
ありがとう
ございました
OK

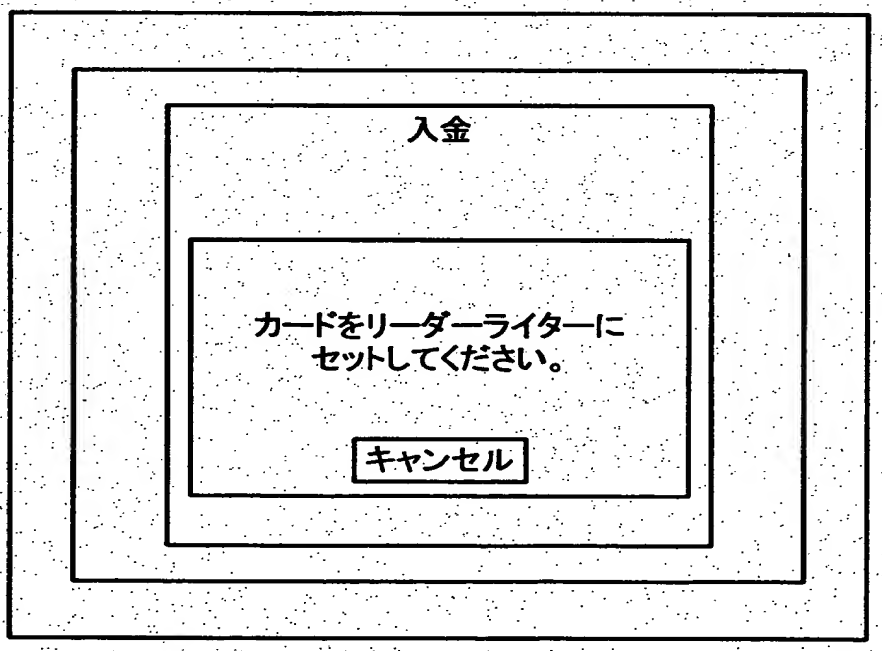
【図２４】


電子マネー入金
精査・決済
システム
32
（バッチ処理）
⑨カードログ情報の送信
30
サイバー電子マネーシステム
⑤クレジット決済要求
④
ログ（カード内
履歴情報）の
吸い上げ
③
入金金額、残高、
クレジットカードNO、
有効期限、
暗証番号送信
②入金画面
⑥価値更新処理
⑦入金完了画面要求
⑧入金完了画面
ユーザ
2
①入金画面要求
35
与信装置

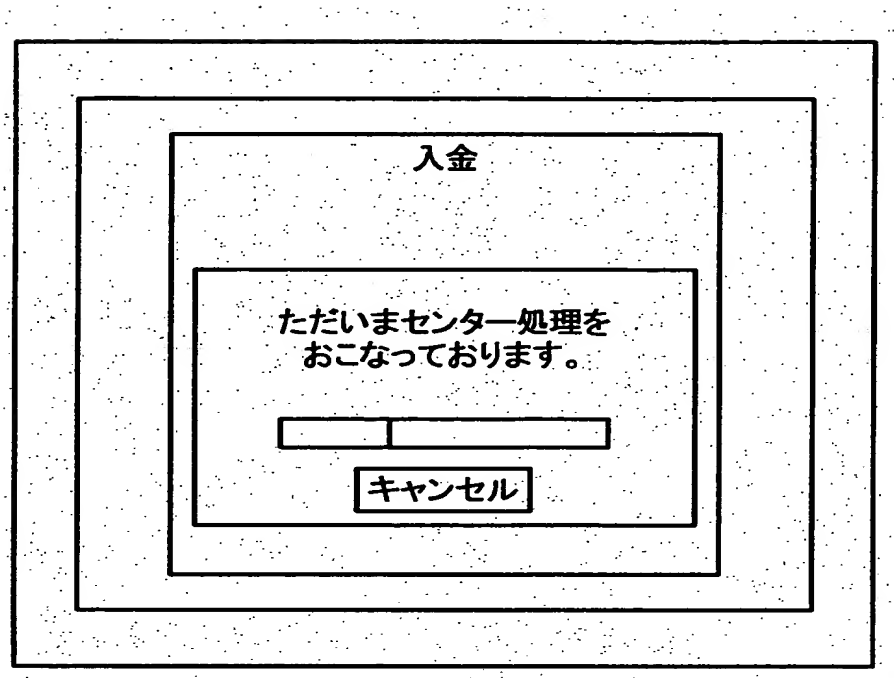
【図２５】


トップページ
サービスを選択してください。
1. 入金
2. 取引履歴表示
3. お問い合わせ

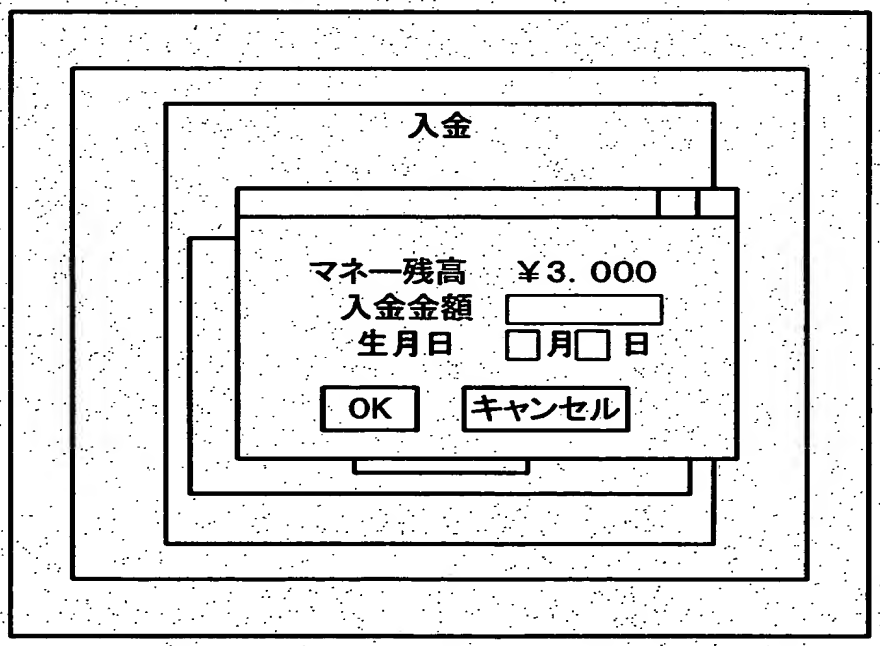
【図２６】


入金
カードをリーダーライターに
セットしてください。
キャンセル

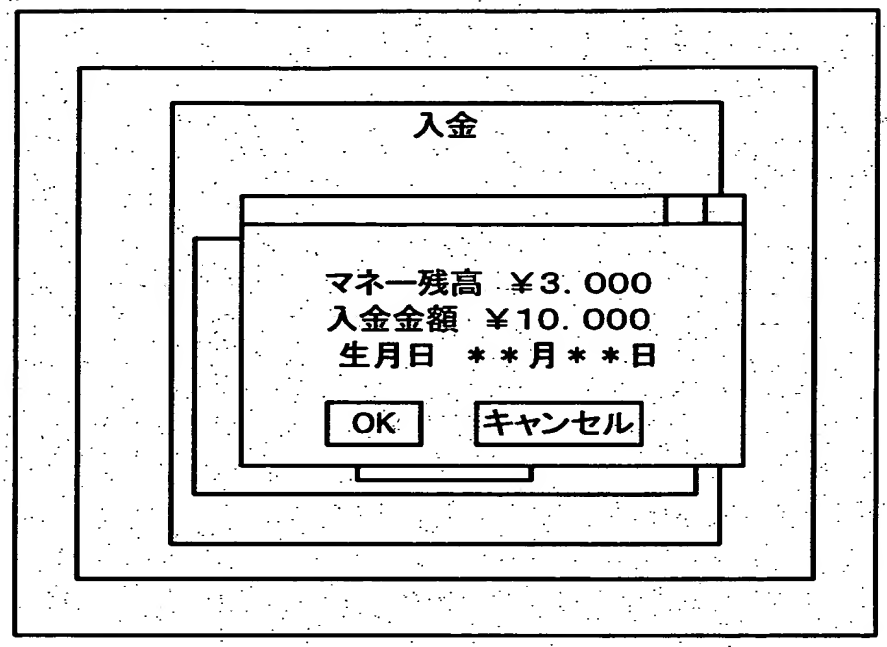
【図２７】


入金
ただいまセンター処理を
おこなっております。
キャンセル

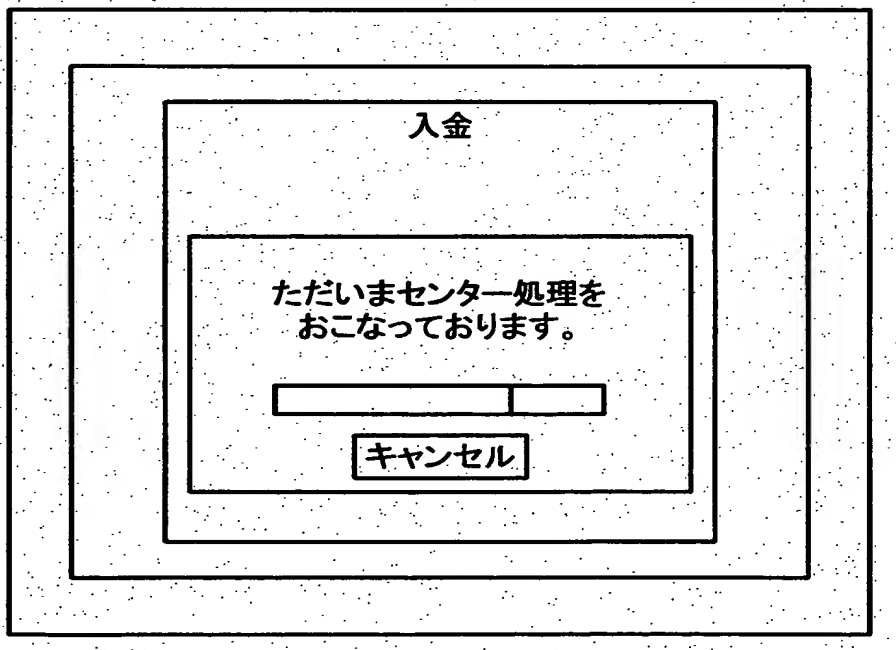
【図２８】


入金
マネー残高 ￥3．000
入金金額
生月日 □月□日
OK
キャンセル

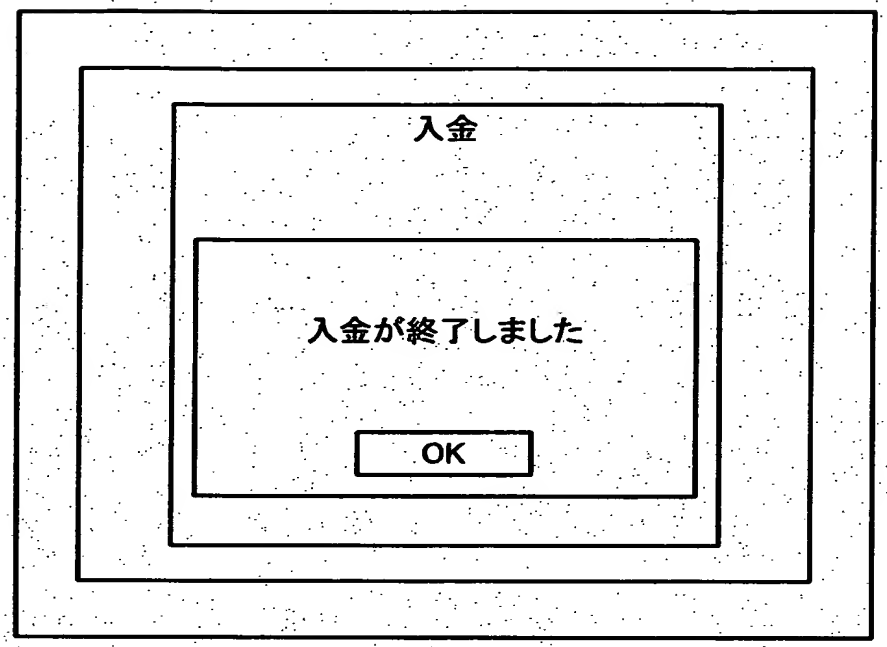
【図２９】


入金
マネー残高 ￥3．000
入金金額 ￥10．000
生月日 ＊＊月＊＊日
OK
キャンセル

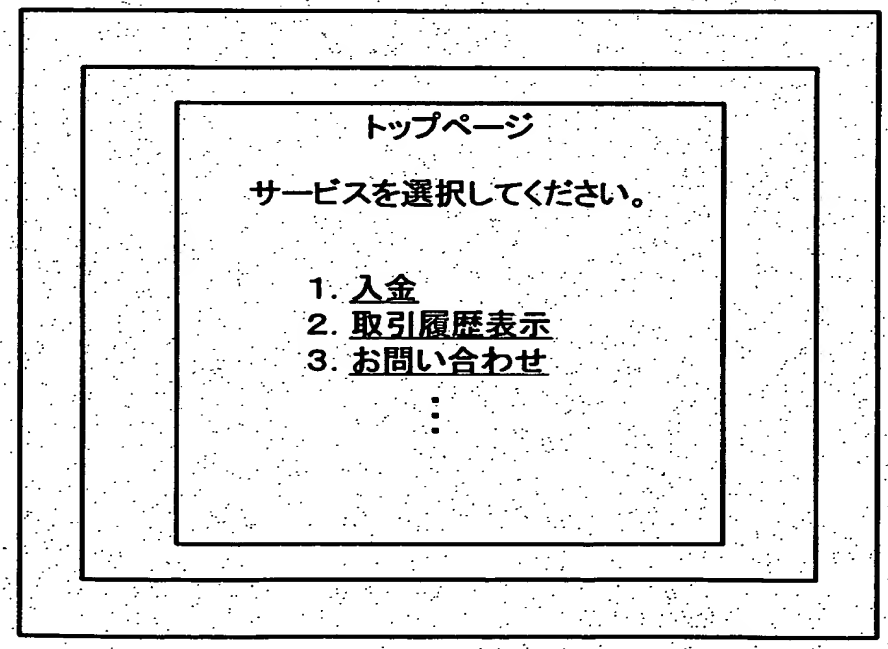
【図３０】


入金
ただいまセンター処理を
おこなっております。
キャンセル

【図３１】



【図３２】



【書類名】　　要約書

【要約】

【課題】　検証回数が少なく効率的な電子決算システムを提供する。

【手段】　電子決算システムは，価値情報が記憶されたＩＣカード２０と，ＩＣカードに対する情報入出力機能を備えたクライアント装置２２と，商品またはサービスを提供する店舗装置４と，ＩＣカードと店舗装置間の決済を管理する決済管理装置３と，クライアント装置と店舗装置と決済管理装置とを双方向通信可能に接続する通信系５とから構成される。決済管理装置は，ＩＣカードで決済を行うための決済情報を，店舗装置からの決済要求情報に基づいて生成し，決済情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化し，この暗号化された決済情報をクライアント装置に送信し，クライアント装置は，決済管理装置から受信した決済情報をＩＣカードに出力することができる。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００１－０４８９１６
受付番号	５０１００２５８２８３
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１３年　２月２８日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100095957
【住所又は居所】	東京都新宿区住吉町１－１２　新宿曙橋ビル　はづき国際特許事務所
【氏名又は名称】	亀谷　美明

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社